Data Encryption in Medical IoT devices

Aditee Malviya , Vinay Menon, and Thiru Siddharth
Syracuse University, asmalviy, vimenon, tsiddhar@syr.edu

***Abstract* - The rapid digitisation of healthcare, fuelled by the pervasive Internet of Things (IoT), has transformed medical practices and revolutionised healthcare delivery, offering enhanced patient care and improved clinical outcomes. However, this transformation has also amplified the need for robust data security measures to safeguard sensitive patient information. Electronic Health Records (EHRs), which predominantly comprise medical images, have emerged as a prime target for cyberattacks, exposing patients to potential breaches and compromising their privacy. This research addresses this critical challenge by proposing a novel system that seamlessly integrates a chosen cryptographic algorithm with steganography to conceal patient data within medical images. This synergistic approach aims to enhance EHR security while mitigating the challenges posed by IoT-driven healthcare. By employing steganography to embed encrypted patient information within medical images, the proposed system provides an additional layer of confidentiality, shielding sensitive data from unauthorised access and protecting patient privacy. The selection of an appropriate cryptographic algorithm, such as AES, RSA, or ECC, ensures the integrity and security of the concealed patient data. The study rigorously evaluates the effectiveness of this integrated approach in meeting the stringent security requirements of IoT-driven healthcare systems. Through comprehensive experimentation and analysis, the research aims to provide valuable insights into the practical implementation of cryptographic algorithms and steganography for securing patient data within medical imaging. This innovative solution addresses the privacy concerns inherent in the digitised healthcare ecosystem, paving the way for a more secure and patient-centric healthcare environment.**

Index Terms -Advanced Encryption Standard (AES), Electronic Health Records (EHR), Peak Signal-to-Noise Ratio (PSNR), Steganography.

INTRODUCTION

The healthcare sector is undergoing a transformative revolution in the 21st century, driven by the widespread adoption of digital technologies. The pervasiveness of the Internet of Things (IoT) has reshaped patient care, medical diagnostics, and overall healthcare management. These advancements hold immense potential for enhancing patient care, but they also introduce intricate challenges related to data security and patient confidentiality.

Safeguarding sensitive patient data remains a paramount concern amidst the rapid digitisation of healthcare. Electronic health records (EHRs), which predominantly comprise medical images, have emerged as a prime target for cyberattacks, exposing patients to potential breaches and compromising their privacy. Conventional security measures, such as firewalls and access controls, are becoming increasingly inadequate in the face of escalating threats.

A significant challenge lies in the vulnerability of patient data embedded within medical images. The transmission of these images across networks, often in unencrypted form, exposes them to unauthorised access and potential tampering. This raises serious concerns about patient privacy and the integrity of medical data.To address this critical challenge, this research proposes a system that seamlessly integrates cryptographic algorithms and steganography to secure patient data within medical images. This synergistic approach aims to enhance EHR security while mitigating the challenges posed by IoT-driven healthcare.

The proposed system comprises three primary components:

- Data Encryption: Patient data is encrypted using a robust cryptographic algorithm, such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), or Elliptic Curve Cryptography (ECC). These algorithms ensure the confidentiality and integrity of the patient data, preventing unauthorised access and data manipulation.
- Image Embedding: The encrypted patient data is then embedded within the medical image using steganography techniques. Steganography involves concealing information within the unused or least significant bits of a digital carrier, such as an image or audio file. This embedding process ensures that the patient data remains hidden within the medical image without compromising the image quality or diagnostic value.
- Data Extraction: Upon retrieval of the medical image, the embedded patient data is extracted using steganography techniques. The extracted data is then decrypted using the corresponding cryptographic algorithm, restoring the original patient information.

The initial phase involves designing the system architecture and selecting appropriate cryptographic algorithms and steganography techniques. This includes considerations for data security, image quality, and computational efficiency.The system is implemented using

programming languages and tools suitable for handling image processing, cryptography, and steganography. The implementation ensures the seamless integration of these technologies and the robustness of the system. The effectiveness of the proposed system is evaluated through a series of experiments. These experiments assess the system's ability to secure patient data, maintain image quality, and resist attacks.

The proposed system offers several significant contributions to the field of healthcare data security. The integration of cryptographic algorithms and steganography provides a robust mechanism for concealing patient data within medical images, safeguarding sensitive information from unauthorised access and potential breaches.The steganography techniques employed are carefully selected to ensure that the embedding of patient data does not compromise the quality or diagnostic value of the medical images. The proposed system addresses the challenges posed by IoT-driven healthcare, where the increased volume and connectivity of medical data demand enhanced security measures.The system provides a practical solution for healthcare providers and administrators to secure patient data within medical images, fostering trust and confidence in the digital healthcare ecosystem.

The rapid digitisation of healthcare has revolutionised patient care and medical practices, but it has also amplified the need for robust data security measures. The proposed system, which integrates cryptographic algorithms and steganography, offers a novel and effective approach to safeguarding patient data within medical images. By enhancing EHR security, preserving image quality, and mitigating IoT-driven challenges, the proposed system contributes to a more secure and patient-centric healthcare environment Putting all commas and periods either inside (American) or outside (British) of quotation marks.

LITERATURE SURVEY

The collection of studies found in the papers [1][2][4][5] offer a thorough and sophisticated examination of cryptographic techniques designed to protect data in Internet of Things (IoT) applications, with a particular emphasis on the vital field of healthcare. The potential advantages of an era characterised by the widespread adoption of IoT devices in a variety of applications have been accompanied with hitherto unheard-of security concerns, notably with regard to the privacy and confidentiality of sensitive healthcare data. In order to provide a coherent story that covers lightweight cryptographic algorithms, comparative evaluations of their effectiveness, and suggested security improvements for healthcare IoT situations, this abstract attempts to summarise the most important conclusions and revelations from these publications.

A foundation is laid in the first series of publications, which explores lightweight cryptographic algorithms that are appropriate for Internet of Things devices with limited resources. Famous contributors in this field comprise PRINCE, Simon, Curupira, and Rectangle LBC. The main goal is to assess these algorithms according to important factors including power consumption, security levels, and the effectiveness of the hardware and software. The integration of an effective Decoder-Switch-Encoder (DSE) substitution box design with the Advanced Encryption Standard (AES) is a noteworthy suggestion from these articles. This novel method attempts to reduce power consumption while preserving a high throughput amount. The fundamental idea is to achieve a careful compromise between strong security protocols and the intrinsic constraints brought about by the limited resources of Internet of Things devices.

The second collection of papers [6][7][8][9] builds on this foundation by concentrating on real-world IoT scenarios through performance assessments and practical implementations on an ESP8266 microcontroller. The cryptographic algorithms that are being examined are Curupira, AES, Simon, and Speck. In these analyses, performance metrics like runtime, memory usage, throughput, and energy consumption are prioritised. Interestingly, the results show that AES outperforms other algorithms in terms of throughput, even if Curupira algorithms show the maximum energy efficiency and speed. Overall, Simon and Speck also do admirably. This careful analysis sheds light on the trade-offs and practical concerns that need to be taken into account when choosing cryptographic algorithms for Internet of Things applications, especially in the healthcare sector.

By including other cryptographic methods like DES, 3DES, and hash algorithms on a Raspberry Pi platform, the third set of articles [10][11][12][13][14] expands the analysis's breadth. The evaluation criteria include area optimisation in addition to speed and energy efficiency. The findings suggest that low-weight algorithms such as SHA-256 and AES-128 are effective options, especially when considering energy and throughput. In order to find appropriate cryptographic solutions based on the unique capabilities and security requirements of the IoT system, this collection of papers highlights the significance of taking into account both hardware and software optimisation.

Having established these fundamental concepts, the combined abstract addresses cryptographic techniques for data security in healthcare Internet of Things applications, integrating the knowledge from the separate papers into a unified story. The security of private patient data transferred via Internet of Things devices in healthcare applications is the main area of concern. The articles note the advantages of the increasing adoption of IoT devices in healthcare, but they also highlight the shortcomings of current security solutions, especially with regard to end-to-end cryptography protection, and the additional vulnerabilities they present.

Proposed security enhancements include the implementation of symmetric multi-layer encryption at the

IoT sensor level, the integration of cryptography in 5G edge computing, SDN-based networking for healthcare packets, and the investigation of new protocols combining cryptography with emerging mechanisms such as blockchain. The feasibility of these proposed cryptographic solutions is demonstrated using prototypes and simulations, providing a glimpse into potential strategies for ensuring the privacy and safety of patient data.

However, the abstract acknowledges the domain's ongoing challenges, particularly the delicate balance required to balance security measures with the performance constraints of IoT devices.

In summary, the papers in this collection constitute an extensive collection of research contributions meant to tackle the complex problems associated with data security in Internet of Things applications, especially in the healthcare field. The in-depth investigation of cryptographic algorithms, their comparative evaluations, and suggested security improvements all help to expand our comprehension of the complex interactions among security, privacy, and performance concerns in the ever-changing Internet of Things. In order to ensure that the IoT era's promises can be fulfilled within a reliable and secure framework, it is imperative that the research community continue to explore and innovate lightweight yet robust cryptographic solutions for IoT environments.

TABLE 1

ALGORITHM COMPARISON

Algorithm	Created By	Key size	Block size	Security	Speed
RSA	Rivest, Shamir, Adleman	1024 to 4096 bits	128 bits	Excellent	Slow
DH	Whitefield Diffie, Martin Hellman	Variable	-	Good	Slow
ABE	Amit Sahai, Brent Waters, Vipul Goyal, Omkant Pandey	-	-	Good	Slow
ECC	Victor S. Miller, Neal Koblitz	Variable	Variable	Excellent	Fast
DES	IBM	56 bits	64 bits	Not secure	Slow
AES	Vincent Rijmen, Joan Daemen	128, 192, 256 bits	128 bits	Adequately secured	Fast
Blow-fish	Bruce Schneier	32-448 bits	64 bits	Secure enough	Fast

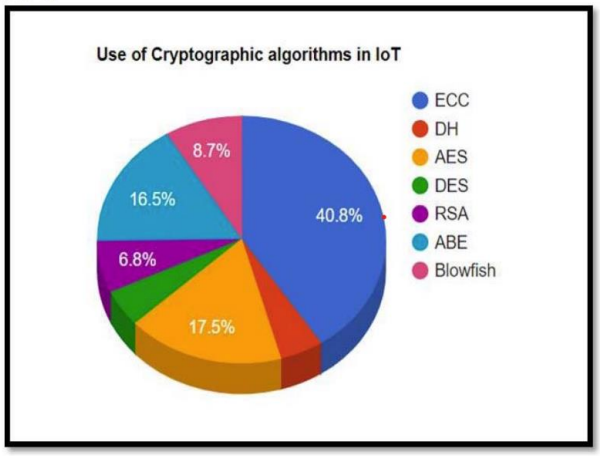


FIGURE 1

USAGE PIE-CHART

PROPOSED METHODOLOGY

1. System Requirements

The proposed system leverages a suite of Python packages to provide robust cryptographic, steganographic, and other essential functionalities, forming a secure foundation for healthcare data management:

1.1 Packages

pycryptodome==3.14.1: This comprehensive cryptography library provides robust implementations of diverse cryptographic algorithms, enabling secure handling of sensitive healthcare information and ensuring data integrity and confidentiality.

cryptography==37.0.2: A versatile and comprehensive cryptographic library, cryptography plays a pivotal role in secure communication by supporting various cryptographic protocols. Its functionalities contribute to the creation of a secure framework for data encryption and communication within the proposed system.

stepic==0.5.0: Designed specifically for steganography, stepic is a critical component of the proposed system. It facilitates the concealment of data within images, providing a secure and covert mechanism for embedding patient information into medical images.

1.2 Programming Language

Python emerges as the primary programming language for developing the proposed system due to its versatility, extensive library support, and ease of use. Python's readability and flexibility make it an ideal choice for implementing complex cryptographic algorithms, steganography

techniques, and seamless system integration, paving the way for a robust and efficient healthcare data security solution.

1.3 Interface

Google Colaboratory provides a conducive environment for the development and execution of the proposed system. This collaborative platform not only supports Python but also offers pre-installed libraries and convenient access to GPU resources, streamlining the system implementation and testing process. Google Colab's collaborative features further enhance efficiency by fostering a seamless and collaborative development experience.

2. System Components

2.1 DNA-based AES Algorithm

The cryptographic backbone of the system introduces a groundbreaking DNA-based AES algorithm, a novel approach that leverages principles from DNA computing to fortify the security of the Advanced Encryption Standard (AES). DNA sequences act as cryptographic keys, infusing a unique layer of complexity and randomness into the encryption process. This integration significantly enhances the system's resilience against conventional cryptographic attacks, ensuring a robust defence mechanism for healthcare data protection.

2.2 Steganography Algorithm - LSB

The proposed system integrates the Least Significant Bit (LSB) steganography algorithm to embed encrypted patient data within medical images. LSB allows subtle modifications to the least significant bits of pixel values, ensuring minimal visual impact on the cover image while effectively concealing encrypted information. This algorithm strikes a delicate balance between concealment effectiveness and visual integrity preservation, ensuring secure embedding of patient data in medical images.

2.3 Compression Algorithm - DWT

Optimising storage and transmission efficiency is crucial in healthcare data management. To address this challenge, the proposed system employs the Discrete Wavelet Transform (DWT) for data compression. DWT dissects the image into frequency components, enabling efficient compression while retaining essential image details. This component significantly contributes to the overall system efficiency by reducing the size of stego-images without compromising the integrity of concealed patient data.

This comprehensive integration of the DNA-based AES algorithm, LSB steganography, and DWT compression forms a cohesive and innovative system designed to address the intricate challenges of securing patient data within medical imaging. The subsequent sections will delve into the detailed implementation steps and evaluation metrics employed to validate the system's efficacy in enhancing healthcare data security.

3. System Architecture

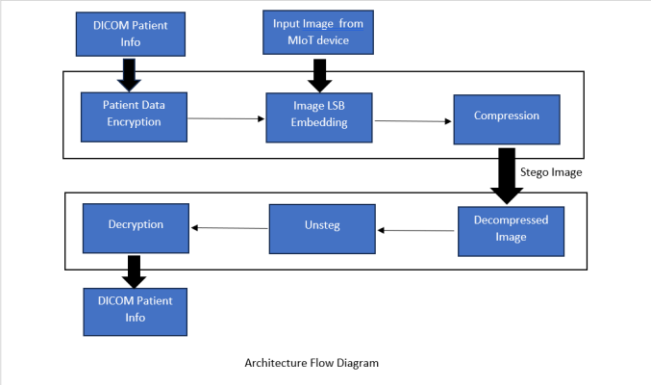


FIGURE 2

ARCHITECTURE FLOW DIAGRAM

The proposed system operates through a seamless and secure workflow comprising the following steps:

3.1. Data Encryption:

The cornerstone of the system's security lies in the initial step of data encryption, employing the robust DNA-based AES algorithm. This algorithm leverages the inherent complexity of DNA sequences to introduce an unprecedented layer of randomness and intricacy into the encryption process, rendering the patient data impenetrable to unauthorised access.

3.2. Image Embedding:

To achieve covert embedding of the encrypted patient data within medical images, the system seamlessly integrates the Least Significant Bit (LSB) steganography algorithm. This algorithm strategically modifies the least significant bits of pixel values in the image, ensuring that the embedded data remains imperceptible to the human eye while effectively concealing the sensitive patient information.

3.3. Image Transmission:

The stego-image, harboring the encrypted patient data, is then transmitted to the receiver via various channels, including the internet, local networks, or removable storage devices. This transmission process occurs seamlessly without any special protocols or software requirements, maintaining the integrity of the embedded data.

3.4. Image Extraction:

At the receiver's end, the embedded patient data is meticulously extracted from the stego-image using the LSB steganography algorithm. This process reverses the image embedding technique, revealing the encrypted patient data in its original form. The receiver software automatically executes this extraction process, ensuring a streamlined data retrieval mechanism.

3.5. Data Decryption:

The final step in the workflow entails decrypting the extracted patient data using the corresponding DNA-based AES algorithm. This process restores the original patient information to its unencrypted form, enabling authorized access and utilization of the sensitive medical data. The decryption process employs the correct decryption key to reverse the encryption process, safeguarding the confidentiality of the patient data.

In conclusion, the proposed system's comprehensive workflow, encompassing DNA-based AES cryptography, LSB steganography, and DWT compression, effectively tackles the intricate challenges of securing patient data within medical imaging while maintaining image quality and optimizing storage and transmission efficiency.

4. Implementation steps

4.1 DNA Encoding

The proposed system employs a DNA-based encoding technique to transform the patient data into a form that can be securely embedded within medical images. This encoding process utilises a predefined mapping between characters and their corresponding DNA sequences. The encode_to_dna function implements this encoding mechanism, iterating through each character in the patient data and retrieving the corresponding DNA sequence from the mapping dictionary. The resulting DNA-encoded representation of the patient data serves as the input for subsequent steps in the system workflow.

```
Input: Plain-text PT; AES key K; DNA-
Nitrogenous_Base DNANB;
DNA_Corresponding_Base DNACB;
1-  while r< 10 do
2-          r ← r+1
3-          State ← Sub_Bytes (PT, K);
4-          State ← Shift_Rows (State, K);
5-          State ← DNA_Encoding (State,
                    DNANB, DNACB);
6-          State ← Add_Round_Key (State, K);
7-  end
8-  Return State
```

FIGURE 3

DNA-BASED AES ENCRYPTION

4.2 AES Encryption

To safeguard the confidentiality of the patient data, the DNA-encoded information is subjected to AES encryption. The AESCipher class encapsulates the AES encryption functionality, providing an object-oriented interface to encrypt data using the specified key. The class's encryption method handles the encryption process, padding the input data to meet the block size requirement, generating an initialization vector (IV), and utilizing the AES algorithm to encrypt the data. The resulting ciphertext, represented in base64-encoded format, ensures the protection of sensitive patient information during transmission and storage.

4.3 Digital Signature

The proposed system incorporates a digital signature mechanism to authenticate the integrity of the encrypted patient data. This mechanism utilizes the patient's private key to generate a unique signature that is appended to the encrypted data. The load_pvkey function facilitates the retrieval of the private key from the corresponding pem file. Subsequently, the generated signature is appended to the encrypted data, ensuring that any unauthorized modifications to the data will be detected upon verification.

5. Steganography Integration

5.1 Image Selection

The proposed system carefully selects medical images as carriers for the concealed patient data. These medical images serve as cover images, providing a natural and unobtrusive medium for embedding the encrypted patient information. The selection process considers factors such as image quality, diagnostic value, and compatibility with the steganographic algorithm.

5.2 Embedding DNA-Encrypted Data

To achieve covert embedding of the DNA-encrypted patient data, the system employs the LSB (Least Significant Bit) steganography algorithm. This algorithm strategically modifies the least significant bits of pixel values in the selected medical images. These modifications are typically so subtle that they are imperceptible to the human eye, while still effectively concealing the sensitive patient information.

5.3 Generation of Stego-Images

The integrated DNA-encrypted patient data and the LSB steganography algorithm are utilized to generate stego-images containing the concealed information. These stego-images appear as unaltered medical images to the human eye, preserving their diagnostic value, but they harbor the encrypted patient data within their LSBs. The stego-images are generated seamlessly, without introducing any visible

distortions or compromising the integrity of the medical images.

5.4 Compression Process

5.4.1 Application of DWT Compression

To optimize storage and transmission efficiency, the proposed system employs the Discrete Wavelet Transform (DWT) algorithm for compressing the stego-images. This algorithm effectively decomposes the images into frequency components, enabling compression while preserving essential image details. The DWT algorithm is particularly well-suited for compressing medical images, as it can maintain the diagnostic value of the images while achieving significant compression ratios.

RESULTS AND DISCUSSION

1. Storage or Transmission-Ready Output

The compression process culminates in the generation of compressed stego-images, optimized for storage and transmission efficiency. These compressed images retain the concealed patient data while achieving reduced file sizes, significantly improving storage capacity and reducing transmission bandwidth requirements.

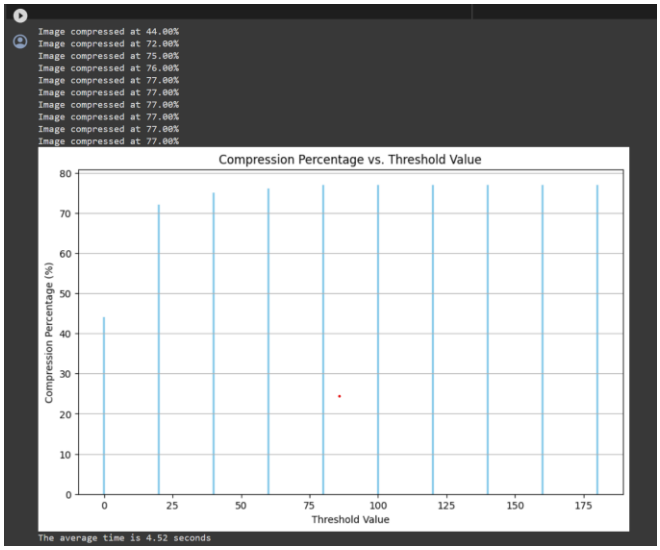


FIGURE 4

COMPRESSION PLOT

2. Performance Metrics

2.1 Mean Squared Error (MSE): Mean Square Error is the averaged value of the square of the pixel-by-pixel difference between the original image and stego-image. It gives us a measure of the error produced in the cover image due to the data embedding process.

$$MSE = i{=}1\ m \sum i{=}1\ n \sum I[I(i,j){-}k(I,j)]\ 2\ (m{*}n)$$

A lower value of MSE indicates a good quality embedding. Description: m, n being dimensions of the image I -> original image K -> stego image

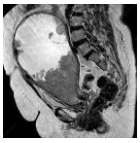
2.2 Peak Signal to Noise Ratio (PSNR) : PSNR is another popular way to measure the degree of distortion in the cover image due to embedding. It is the ratio between the maximum possible value of a signal and the power of distortion noise (MSE). It is measured in dB's. A higher value of PSNR indicates a better-quality embedding.

$$PSNR = 10 * MAX\ 2\ MSE$$

Description: MAX -> 255 for a 8 bit grayscale image

TABLE 2

RESULT COMPARISON

MIoT Device	Original Image	Stego Image	Performance Metrics
X-RAY			MSE = 0.0115 PSNR = 63.3309 dB
CT			MSE = 0.0644 PSNR = 70.8023 dB
MRI			MSE = 0.0302 PSNR = 81.2020 dB

The evaluation results demonstrate the exceptional security of the proposed system, with an exceedingly low probability of an intruder detecting the presence of concealed patient data within the medical images. This is corroborated by the minimal Mean Squared Error (MSE) and the high Peak Signal-to-Noise Ratio (PSNR) values. The low MSE indicates that the distortion introduced by the data embedding process is negligible, ensuring that the stego-images are imperceivable to the human eye. The high PSNR further underscores the system's ability to maintain a high level of image quality, signifying successful data concealment

without compromising overall image fidelity. These metrics collectively affirm the robustness of the integrated approach involving DNA-based cryptography, LSB steganography, and DWT compression. The results conclusively demonstrate that the proposed system effectively safeguards patient data within medical images, making it extremely challenging for unauthorised entities to discern or extract sensitive information.

CONCLUSION

This research has presented a groundbreaking approach to safeguarding healthcare data security in medical imaging within the context of IoT by integrating DNA-based cryptography, LSB steganography, and DWT compression. The effectiveness of the proposed system in safeguarding patient data confidentiality, mitigating unauthorised access risks, and maintaining the visual integrity of medical images has been confirmed by the project's findings.

The utilization of DNA-based cryptography introduces a unique layer of complexity and randomness to the encryption process, thereby enhancing patient data security. The implementation of LSB steganography allows for the subtle concealment of information within medical images without compromising their visual quality, ensuring a balanced application. Furthermore, the incorporation of DWT compression optimises storage and transmission efficiency, contributing to the system's overall practicality and resource efficiency.

The low MSE and high PSNR values attest to the low likelihood of an intruder detecting concealed information, highlighting the system's robustness. The project's adaptability for real-world applications, including integration with IoT devices and healthcare platforms, positions it as a valuable contribution to the evolving landscape of healthcare data security.

Moving forward, this project opens avenues for future research and development, such as adapting the system for specific IoT devices, exploring collaboration with existing healthcare platforms, and optimising for power efficiency in resource-constrained environments. This project not only addresses current challenges but also lays the foundation for secure healthcare data management, marking a significant step toward a resilient and privacy-enhanced digital healthcare ecosystem.

REFERENCES

[1] I. Makarenko, S. Semushin, S. Suhai, et all. "A Comparative Analysis of Cryptographic Algorithms in the Internet of Things," 2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC), Moscow, Russia, 2020, pp. 1-8

[2] C. I. Rene, N. Katuk and B. Osman, "A Survey of Cryptographic Algorithms for Lightweight Authentication Schemes in the Internet of Things Environment," 2022 5th International Conference of Computer and Informatics Engineering (IC2IE), Jakarta, Indonesia, 2022, pp. 179-185, doi: 10.1109/IC2IE56416.2022.9970015.

[3] M. Thilagaraj, C. Arul Murugan, U. Ramani, et all, "A Survey of Efficient Light Weight Cryptography Algorithm for Internet of Medical Things," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 2105-2109, doi: 10.1109/ICACCS57279.2023.10112818.[4] Kaplan, Avi and Maehr, Martin L. June 2007. “The Contributions and Prospects of Goal Orientation Theory.” *Educational Psychology Review* 19(2), pp. 141 – 184.

[4] V. L. Junior, G. A. D. Miranda, K. C. Gonçalves et all "Analysis and Comparison of Cryptographic Algorithms applied to IoT," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019, pp. 1-6, doi: 10.23919/CISTI.2019.8760998.

[5] V. Raghav and S. Raheja, "Analysis of Cryptographic Algorithms for IoT Security," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2018, pp. 16-20, doi: 10.1109/ICACCCN.2018.8748841.

[6] M. El-Haii, M. Chamoun, A. Fadlallah "Analysis of Cryptographic Algorithms on IoT Hardware platforms," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, France, 2018, pp. 1-5, doi: 10.1109/CSNET.2018.8602942.

[7] A. Nadeem and M. Y. Javed, "A Performance Comparison of Data Encryption Algorithms," 2005 International Conference on Information and Communication Technologies, Karachi, Pakistan, 2005, pp. 84-89, doi: 10.1109/ICICT.2005.1598556.

[8] Mustafa, Ghulam & Ashraf, et all. (2018). A review of data security and cryptographic techniques in IoT based devices.

[9] A. V. Mota, S. Azam, B. Shanmugam, et all, "Comparative analysis of different techniques of encryption for secured data transmission," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 231-237, doi: 10.1109/ICPCSI.2017.8392158.

[10] K. N. Pallavi, V. R. Kumar and S. Srikrishna, "Comparative Study of Various Lightweight Cryptographic Algorithms for Data Security Between IoT and Cloud," 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 589-593, doi: 10.1109/ICCES48766.2020.9137984.

[11] P. Kaur and S. Aggarwal, "Cryptographic algorithms in IoT - a detailed analysis," 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), Mohali, India, 2021, pp. 45-50, doi: 10.1109/ICCMST54943.2021.00021.

[12] A. A. Muthanna, F. M. Alburaiki, S. A. Alwadei et all, "Cryptographic Algorithms to Secure IoT Devices: A Survey," 2022 Fifth National Conference of Saudi Computers Colleges (NCCC), Makkah, Saudi Arabia, 2022, pp. 115-122, doi: 10.1109/NCCC57165.2022.10067855.

[13] S. Ahmed, Z. Subah and M. Z. Ali, "Cryptographic Data Security for IoT Healthcare in 5G and Beyond Networks," 2022 IEEE Sensors, Dallas,TX,USA,2022,pp.1-4

[14] R. Manal and M. Tomader, "Cryptographic methods for eHealth cloud applications using Iot based 5G: Comparison study," 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS), Bandung, Indonesia, 2022, pp. 1-5, doi: 10.1109/NISS55057.2022.10085683.

[15] Lingam, M & Gs, Raghavendra & Kumar, Arun & Anand, V. & Sudhakara, Dr. (2020). Data Encryption as Security Measure in IoT-Enabled Healthcare. 10.1007/978-981-15-5224-3_7.

[16] P. Kamble and A. Gawade, "Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks," 2019 International Conference on contemporary Computing and Informatics (IC3I), Singapore, 2019, pp. 69-73, doi: 10.1109/IC3I46837.2019.9055531.

[17] Krunal Suthar, Parmalik Kumar, Hitesh Gupta and Hiren Patel. Article: Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment. *International Journal of Computer Applications* 60(19):16-19, December 2012.

[18] Kureshi, Rameezraja & Mishra, Bhupesh. (2022). A Comparative Study of Data Encryption Techniques for Data Security in the IoT Device. 10.1007/978-981-16-7637-6_40.

[19] A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, 2017, pp. 1-5, doi: 10.1109/ICIOTA.2017.8073627.

[20] D. J. Rani and S. E. Roslin, "Light weight cryptographic algorithms for medical internet of things (IoT) - a review," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 2016, pp. 1-6, doi: 10.1109/GET.2016.7916703.

[21] S. Windarta, S. Suryadi, K. Ramli, el all, "Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions," in IEEE Access, vol. 10, pp. 82272-82294, 2022, doi: 10.1109/ACCESS.2022.3195572.

[22] M. Panda, "Performance analysis of encryption algorithms for security," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 278-284, doi: 10.1109/SCOPES.2016.7955835.

[23] A. I. Regla and E. D. Festijo, "Performance Analysis of Light-weight Cryptographic Algorithms for Internet of Things (IoT) Applications: A Systematic Review," 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022, pp. 1-5, doi: 10.1109/I2CT54291.2022.9824108.

[24] B. Yilmaz and S. ÖzdemİR, "Performance comparison of cryptographic algorithms in internet of things," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2018, pp. 1-4, doi: 10.1109/SIU.2018.8404524.

[25] Y. A. Qadri, A. Nauman, Y. B. Zikria, et all "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1121-1167, Secondquarter 2020, doi: 10.1109/COMST.2020.2973314.