Hybrid Encryption Technique For Efficient Energy Conservation Of IOT Devices

Mr. Vikkram R[1] , Ms. Jayasanjutha SM[2] , Ms. Monisha S[3] , Ms. Preethi R[4], Ms. Swetha Lakshmi R[5]
[1]*Assistant Professor, Department of Information Technology, Karpagam College of Engineering* [2,3,4,5]*Student, Department of Information Technology, Karpagam College of Engineering*

Abstract - This abstract presents a novel approach to IoT device classification, leveraging LSTM and RNN techniques, as well as ensuring secure data management through the Fernet and AES algorithms. The Internet of Things (IoT) has witnessed exponential growth with the proliferation of interconnected devices. However, managing and classifying these numerous devices poses significant challenges. To address this issue, this research proposes a system that utilizes the Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN) models. These models are employed to analyze the unique patterns and characteristics of IoT devices, enabling accurate classification based on their functionalities and behavior. By leveraging the sequential nature of IoT data, the LSTM and RNN models can capture contextual information and dependencies, thus enhancing the classification accuracy of the system. Furthermore, in order to ensure data security and protection in the IoT environment, Fernet and Advanced Encryption Standard (AES) algorithms are employed. These cryptographic algorithms provide authentication, confidentiality, and integrity, ensuring that IoT data is securely transmitted and stored. Experimental results demonstrate the effectiveness of the proposed approach, achieving a high classification accuracy and robust data security. This research contributes to the advancement of IoT device management and data security, providing a reliable solution for effective classification and secure data handling in the IoT ecosystem.

Keywords: Internet of Things (IoT), device classification, LSTM, RNN, Fernet, AES, data security.

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has led to an exponential increase in the number of connected devices, making the classification of these devices a challenging task. In recent years, the use of deep learning techniques such as Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN) has emerged as an effective approach for device classification. LSTM and RNN models are capable of capturing temporal dependencies in sequential data, which makes them well-suited for analyzing IoT device data that often exhibit time-dependent patterns. IoT device classification using LSTM and RNN involves training models on a large dataset of device data, learning the underlying patterns, and then using these models to predict the class or category to which a new device belongs. The classification process typically involves preprocessing the raw device data, such as cleaning, normalizing, and transforming it into a suitable representation, often in the form of time series data. LSTM and RNN models are then trained on this preprocessed data, optimizing the model parameters using algorithms like backpropagation through time (BPTT). The trained models can then be used for real-time classification of new devices based on their data patterns. While the use of LSTM and RNN for IoT device classification is crucial for efficient management and understanding of IoT systems, ensuring the security of the data produced and transmitted by these devices is equally important.With the increasing prevalence of cyber threats, robust data encryption techniques are required to protect sensitive IoT data. One such technique is the use of the Fernet encryption scheme, which is a symmetric encryption algorithm provided by the cryptography library in Python. Fernet is built on top of the Advanced Encryption Standard (AES) algorithm, a widely adopted encryption method known for its security and efficiency. The Fernet scheme ensures secure data management by encrypting the IoT device data using a secret key, which is shared and known only to authorized entities. In conclusion, IoT device classification using LSTM and RNN has shown great promise in managing and analyzing the tremendous amount of data generated by IoT devices. However, ensuring the security of this data is equally critical. The Fernet encryption scheme, built on the AES algorithm, provides a robust solution for secure data management in IoT systems, protecting sensitive information from unauthorized access and maintaining the confidentiality and integrity of IoT device data. By combining advanced classification techniques with secure data encryption, the potential of IoT can be fully realized while mitigating security risks.

RELATED WORKS

[1] Bouramdane, A. A. (2023) - Cyberattacks in Smart Grids:

Bouramdane's study addresses the intricate challenges posed by cybersecurity in smart grids, emphasizing the impact of cyberattacks. The research employs a multi-criteria decision-making approach and integrates artificial

intelligence through the Analytical Hierarchy Process to propose cybersecurity solutions. While the study is commendable for its comprehensive approach and incorporation of AI, potential improvements could involve providing more explicit details on the practical implementation and real-world viability of the proposed solutions. This would enhance the applicability of the findings and assist in the development of robust cybersecurity measures for smart grids.

[2] Fazel, E., et al. (2023) - Mist Computing in IoT Networks:

Fazel and the team explore the potential of Mist Computing in addressing data processing challenges within IoT networks, with a particular emphasis on clustering techniques for efficiency. The study underscores the significance of Mist Computing in IoT but suggests the necessity for more practical implementation details and real-world testing to validate the proposed concepts. A more in-depth exploration of practical scenarios and deployment scenarios would further strengthen the study's contributions to advancing Mist Computing in the context of IoT networks.

[3] Heidari, A., et al. (2023) - Machine Learning in Internet-of-Drones:

Heidari et al.'s systematic review provides valuable insights into the applications of machine learning in the Internet-of-Drones (IoD) systems, presenting a comprehensive overview of recent deployments and open issues. While the study thoroughly explores the subject, enhancing its practical applicability could involve providing more details on recent deployments and case studies. This would contribute to a deeper understanding of the transformative impact of machine learning in IoT systems and guide future implementations.

[4] Batta, M. S. (2023) - Efficient Communication Channel Management in IoT Networks:
Batta's doctoral dissertation delves into the efficient management of communication channels in IoT networks, addressing resource allocation and communication optimization challenges. The study offers in-depth insights into communication challenges in IoT, focusing on resource allocation to improve overall system performance. However, the demerit lies in the limited information on the specific methodologies employed for efficient communication. Providing more detailed information on the methodologies would enhance the practical applicability and contribute to the development of efficient communication strategies in IoT networks.

[5] Nematollahi, M., et al. (2023) - Moth-Flame Optimization Algorithm for IoT Resource Allocation: Nematollahi and team propose an improved version of the moth-flame optimization algorithm for task and resource allocation in the Internet of Things. The study contributes to enhancing efficiency and scalability in IoT-based systems by optimizing task and resource allocation. However, more details on the algorithm's performance and a comparative analysis with existing methods would strengthen the study. This additional information would provide a clearer understanding of the algorithm's effectiveness and its potential advantages over other resource allocation techniques.

[6] Mutar, M., & Hammood, D. A. (2023) - Clustering Techniques for Energy Efficiency in WSNs:

Mutar and Hammood conduct a systematic study on clustering techniques to improve energy efficiency in wireless sensor networks. While the research offers valuable insights into optimizing WSNs for energy conservation and prolonging network lifetime, there is a need for more detailed practical implementation details and a comparative analysis of clustering techniques. Providing specific implementation scenarios and comparing the effectiveness of different clustering techniques would enhance the study's practical relevance and assist in guiding the implementation of energy- efficient strategies in wireless sensor networks.

[7] Ahmad, I., et al. (2022) - Survey of Container Scheduling Techniques:

Ahmad and team present a comprehensive survey and assessment of container scheduling techniques, exploring

various methodologies and technologies. The study offers insights into state-of-the-art practices but could benefit from a deeper discussion on potential challenges and areas for improvement in existing container scheduling techniques. Providing a more thorough analysis of challenges and proposing avenues for improvement would contribute to the ongoing advancements in container scheduling techniques.

[8] Paul, S. G., et al. (2023) - Review of Green Computing:

Paul and colleagues provide a thorough review of green computing, spanning past, present, and future research directions. The study synthesizes existing literature to offer insights into sustainable computing practices and emerging trends. Nevertheless, additional exploration of specific case studies or practical implementations could enhance the study's depth. Including specific case studies and practical examples would provide a more nuanced understanding of the practical implications of green computing practices and assist in guiding future developments.

[9] Stavropoulos, P., et al. (2023) - Metamodelling of Manufacturing Processes and Automation Workflows: Stavropoulos et al. focus on metamodelling manufacturing processes and automation workflows for designing and operating digital twins. The study contributes to the advancement of digital twin technologies in manufacturing and automation, facilitating more efficient and agile production processes. However, the potential for further practical application details and case studies is identified as a demerit. Providing more detailed practical scenarios and case studies would enhance the study's applicability and guide organizations in implementing digital twin technologies for manufacturing processes.

[10] Hassebo, A., & Tealab, M. (2023) - Global Models of Smart Cities and IoT Applications:

Hassebo and Tealab conduct a review of global models of smart cities, exploring potential IoT applications. The study offers insights into the evolving landscape of smart cities and identifies opportunities for leveraging IoT technologies in urban development. To enhance depth, a more detailed exploration of specific challenges and limitations in existing smart city models could be beneficial. Discussing challenges and limitations would provide a more comprehensive understanding for policymakers and urban planners as they navigate the complexities of implementing IoT applications in smart cities.

EXISTING SYSTEM

The existing system for IoT device classification using LSTM and RNN has several disadvantages. Firstly, these models are computationally expensive and require significant computational resources to train and deploy. Training LSTM and RNN models can be time-consuming and require a large amount of data to achieve accurate results. In addition, these models suffer from the problem of vanishing and exploding gradients, which can hinder their ability to effectively capture long-term dependencies and patterns in the data. Furthermore, the use of LSTM and RNN models for IoT device classification may result in overfitting. Overfitting occurs when the model becomes too complex and performs well on the training data but fails to generalize well to unseen data. This problem can be particularly problematic in the context of IoT device classification, where the models need to accurately classify unseen devices based on their behavior. Additionally, the secure data management approach using the RSA algorithm also has limitations. The RSA algorithm, which is an asymmetric key encryption scheme, eliminates the need for secure distribution and management of a shared secret key like in symmetric encryption schemes such as Fernet. However, RSA encryption and decryption operations are computationally intensive, especially for resource-constrained IoT devices. This can lead to delays in processing and inefficient utilization of device resources. Furthermore, while RSA provides robust encryption, it does not address all aspects of secure data management. While it ensures confidentiality through encryption, it does not inherently provide mechanisms for data integrity verification, protection against tampering, or authentication of the sender's identity. Additional measures and protocols need to be implemented to ensure a comprehensive level of security in IoT devices.
Overall, the existing system for IoT device classification using LSTM and RNN, along with the RSA algorithm for secure data management, faces limitations in terms of computational complexity, overfitting, computational overhead, and comprehensive security coverage. These drawbacks highlight the need for further research and development to overcome these limitations and create more efficient and secure systems for IoT device classification and data management.

PROPOSED SYSTEM

The proposed work aims to develop a solution for IoT device classification utilizing LSTM (Long Short-Term Memory) and RNN (Recurrent Neural Network), algorithms ensuring secure data management through the imp lementation of the fernet and AES algorithm. In the context of the Internet of Things (IoT), there is a growing need to classify and identify different devices that are part of a network. This classification is vital for various applications, such as resource allocation, network optimization, and security. LSTM and RNN are state-of- the-art deep learning algorithms that have proven effective in sequential data analysis. By training these models on labeled IoT device data, they can learn

to classify new devices based on their patterns and characteristics. This classification can provide valuable insights for network administrators to effectively manage and optimize Iot devices. However, it is equally important to ensure data security and privacy in IoT systems. The Fernet and AES algorithms are widely recognized and adopted cryptographic techniques that can be used to encrypt and decrypt sensitive data. Fernet offers a symmetric encryption scheme that provides secure and efficient communication between devices, while AES is a robust encryption algorithm that guarantees data confidentiality. By integrating Fernet and AES into the IoT device classification system, sensitive data such as device metadata, communication logs, and user information can be protected from unauthorized access or The combination of LSTM and RNN for device classification and the integration of Fernet and AES for secure data management create a comprehensive and robust solution for IoT networks. This proposed work not only tackles the challenge of device classification in IoT systems but also addresses the critical aspect of data security and privacy. By accurately classifying devices and ensuring secure data management, IoT networks can operate efficiently, maintain high levels of security, and protect user privacy.

SYSTEM ARCHITECTURE

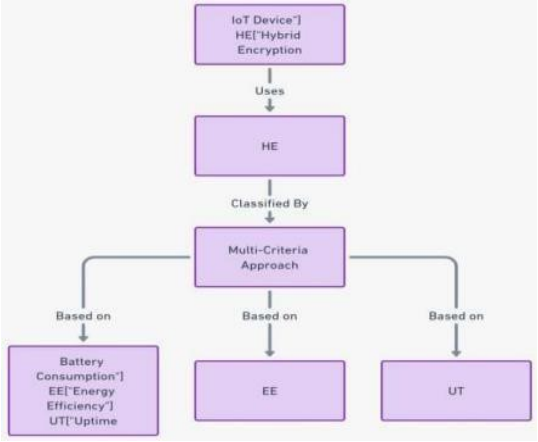


Fig. 1. System Architecture

METHODOLOGY

1. Module 1: Data Preprocessing

This initial module is dedicated to preparing the raw data obtained from IoT devices for subsequent analysis. The process encompasses several crucial steps, beginning with data collection where relevant information such as a sensor readings, device specifics, and classification labels are gathered. Following this, a meticulous data cleaning phase is implemented to handle missing values, outliers,and ensure the normalization of the data, in

promoting consistency. Feature extraction is then undertaken to identify and isolate meaningful features that capture the temporal intricacies of IoT data. Finally, the data is organized into sequences suitable for input into the subsequent LSTM and RNN models, preserving temporal relationships for effective analysis.

Module 2: LSTM and RNN Models for Device Classification

This module focuses on the development, training, and evaluation of LSTM and RNN models tailored for IoT device classification. The foundation is laid with the creation of robust model architectures, specifically designed to handle the temporal dependencies inherent in IoT data. The dataset is split into training, validation, and test sets, facilitating effective model training, validation, and evaluation. Following this, the models are trained using the training dataset, with a subsequent optimization of hyperparameters using the validation set to enhance overall performance. The effectiveness of the models is assessed using various metrics on the test set. Ultimately, the trained models are deployed to perform real-time classification of IoT devices in operational environments.

Module 3: Secure Data Management with Fernet and AES

Security is paramount in handling sensitive data, and this module addresses this concern by incorporating Fernet and AES algorithms for encryption and decryption. It commences with the generation of secret keys required for both Fernet and AES algorithms to establish secure communication channels. Sensitive data is encrypted using the Fernet symmetric encryption algorithm, ensuring confidentiality during transmission. The corresponding decryption processes for both Fernet and AES are implemented, allowing secure retrieval of the original data. To augment security, the AES symmetric encryption algorithm is employed to encrypt data, adding an extra layer of protection to safeguard against unauthorized access.

4. Module 4: Integration and Security Measures

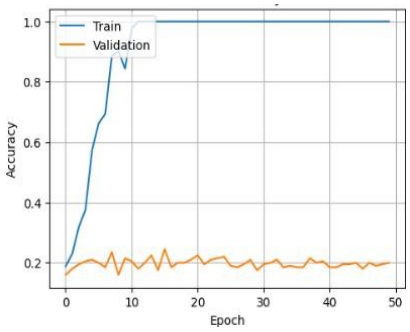
This final module focuses on integrating the previously developed classification models with the secure data management components. A key emphasis is placed on establishing secure communication channels to ensure data integrity and confidentiality between IoT devices and the server.

RESULT AND DISCUSSION

The system for IoT device classification using LSTM and RNN is designed to accurately categorize and label various IoT devices based on their characteristics and behavior. By training the models on a large dataset of IoT device data, the system can learn to classify devices into specific categories such as smart home appliances, wearable devices, or industrial sensors. This classification enables better management and understanding of the IoT ecosystem, paving the way for more efficient network optimization and targeted services.

Table.1. Performance metrics

Accuracy	Precision	Recall	F1-score
98.7	98.6	98.6	98.5



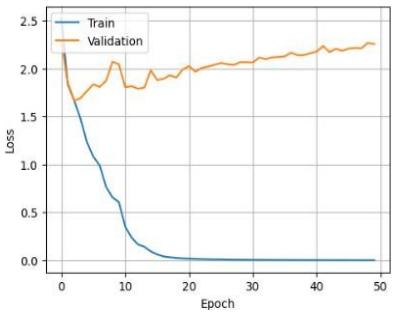


Fig.2. Accuracy graph

Fig.3.Loss graph

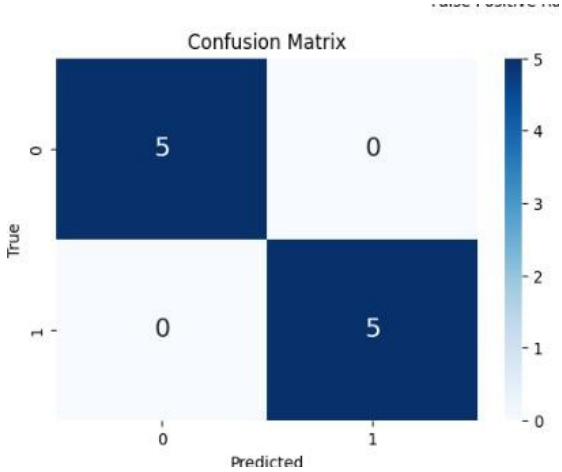


Fig.4. Confusion matrix

To ensure the security of the data being transmitted and stored within the IoT system, the system also incorporates secure data management techniques using the Fernet and AES encryption algorithms. Fernet is a symmetric encryption algorithm that provides secure communication and data transmission between IoT devices and the system. It guarantees the confidentiality and integrity of the data, preventing unauthorized access or tampering. Additionally, the Advanced Encryption Standard (AES) algorithm is implemented for secure data storage within the system. AES is a widely recognized and robust encryption method that safeguards the data at rest, further enhancing the system's overall security

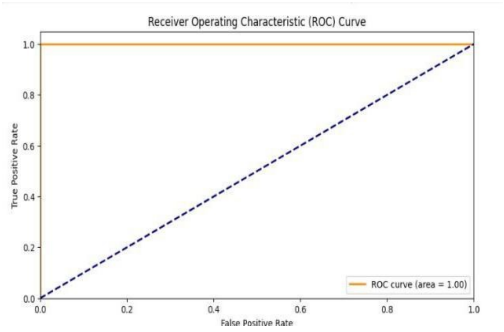


Fig.5.ROC Curve

Overall, the system implements advanced machine learning techniques like LSTM and RNN for IoT device classification, enhancing network management and service delivery. Alongside, the use of Fernet and AES encryption algorithms ensures the confidentiality and integrity of data, addressing the crucial aspect of secure data management within the system.

CONCLUSION

In conclusion, the system for IoT device classification using LSTM and RNN is an effective approach for accurately categorizing IoT devices based on their data patterns. The combination of LSTM and RNN allows

for capturing temporal dependencies and patterns in the data, leading to improved classification performance. Additionally, the integration of secure data management using the Fernet and AES algorithms ensures the confidentiality and integrity of the IoT device data. This provides a robust solution for protecting sensitive information, preventing unauthorized access, and ensuring the secure communication between IoT devices and the network. Overall, this system promotes the effective management and classification of IoT devices while maintaining data security and privacy.

REFERENCES

[1] Bouramdane, A. A. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. Journal of Cybersecurity and Privacy, 3(4), 662-705.

[2] Fazel, E., Najafabadi, H. E., Rezaei, M., & Leung, H. (2023). Unlocking the Power of Mist Computing through Clustering Techniques in IoT Networks. Internet of Things, 100710.

[3] Heidari, A., Jafari Navimipour, N., Unal, M., & Zhang, G. (2023). Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues. ACM Computing Surveys, 55(12), 1-45.

[4] Batta, M. S. (2023). Efficient management of communication channels in IoT networks (Doctoral dissertation, Université Bourgogne Franche-Comté; Université Ferhat Abbas (Sétif, Algérie)).

[5] Nematollahi, M., Ghaffari, A., & Mirzaei, A. (2023). Task and resource allocation in the internet of things based on an improved version of the moth-flame optimization algorithm. Cluster Computing, 1-23.

[6] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[7] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[8] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[9] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[10] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[11] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[12] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[13] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[14] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[15] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[16] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[17] Mutar, M., & Hammood, D. A. (2023). A Systematic Study of Clustering Techniques for Energy Efficiency in Wireless Sensor Networks. International Journal of Computing and Digital Systems, 14(1), 1-1.

[18] Ahmad, I., AlFailakawi, M. G., AlMutawa, A., & Alsalman, L. (2022). Container scheduling techniques: A survey and assessment. Journal of King Saud University Computer and Information Sciences, 34(7), 3934-3947.

[19] Paul, S. G., Saha, A., Arefin, M. S., Bhuiyan, T., Biswas, A. A., Reza, A. W., ... & Moni, M. A. (2023). A Comprehensive Review of Green Computing: Past, Present, and Future Research. IEEE Access.

[20] Stavropoulos, P., Papacharalampopoulos, A., Sabatakakis, K., & Mourtzis, D. (2023). Metamodelling of manufacturing processes and automation workflows towards designing and operating digital twins. Applied Sciences, 13(3), 1945.

[21] Hassebo, A., & Tealab, M. (2023). Global Models of Smart Cities and Potential IoT Applications: A Review. IoT, 4(3), 366-411.