ENHANCE DEEP FAKE DETECTION IN VIDEOS USING LONG SHORT TERM MEMORY WITH DISTRIBUTED COMPUTING

A THESIS

A Partial Requirement to Fulfill for Master Degree in Computer Science

ALEYK FATKHUNNAJAKHI
NIM : 20210130030

Supervisor:
Prof. Teddy Mantoro, MSc., PhD., SMIEE
Harris Al qodri Maarif, S.T., M.Sc., Phd

SCHOOL OF COMPUTER SCIENCE
NUSA PUTRA UNIVERSITY
2024

STATEMENT OF AUTENTICITY

The undersigned below:

Name : ALEYK FATKHUNNAJAKHI

ID of student : 20210130030

Faculty : Computer Science

The Tittle of Thesis : Enhance Deep Fake Detection in Videos Using Long Short Term Memory with Distributed Computing

Stating truthfully that this thesis has nothing in common with other thesis. Thus this statement is made without coercion from any party. If this statement is not true, it will be sanctioned by the faculty leader.

Sukabumi, Juli 2024

Writer,

Materai 10000

Aleyk Fatkhunnajakhi

20210130030

APPROVAL OF THESIS

The Tittle of Thesis : Enhance Deep Fake Detection in Videos Using Long Short Term Memory with Distributed Computing

Name : Aleyk Fatkhunnajakhi

ID of student : 20210130030

This thesis has been reviewed and approved

Sukabumi, November 2023

Head of Study Program,	Supervisors,
Prof. Ir. Teddy Mantoro, M.Sc., PhD.	Prof. Ir. Teddy Mantoro, M.Sc., PhD.
NIDN. 0323096491	NIDN. 0323096491

THESIS APPROVAL

The Tittle of Thesis : Enhance Deep Fake Detection in Videos Using Long Short Term Memory with Distributed Computing

Name : Aleyk Fatkhunnajakhi

ID of student : 20210130030

This Thesis has been tested and defended in front of the Board of Examiners in

Thesis session on November 19, 2023. In our review, this Thesis adequate in terms of quality for the purpose of awarding the Master of Computer Degree.

Supervisor 1	Examiner 1
Prof. Ir.Teddy Mantoro, MSc., PhD., SMIEEE	Mr. Umar Aditiawarman, S.T., M.Sc., PhD
NIDN. 0323096491	

Supervisor 2	Examiner 2

PUBLICATION APPROVAL

As a member of the academic community of Nusa Putra University I undersigned:

Name	: Aleyk Fatkhunnajakhi
ID of student	: 20210130030
Study Program	: Computer Science
Type of Work	: Thesis

For the sake of scientific development, agree to grant to the University of Nusa Putra the Non-Exclusive Royality-Free Right for my scientific work entitled: **Enhance Deep Fake Detection in Videos Using Long Short Term Memory with Distributed Computing**. With this non-exclusive royalty-free right, Nusa Putra University has the right to store, transfer media/formats, process in the form of a database, maintain and publish my thesis as long as I keep my name as the author/creator and as the copyright owner. This statement I made in truth.

Made in: Sukabumi

At the Date of: November 2023

(Aleyk Fatkhunnajakhi)

LIST OF CONTENT

LIST OF FIGURE

LIST OF TABLE

FOREWORD

All praises to Allah SWT for His infinite mercy and guidance, enabling the author to complete this Thesis with the title "Malware Classification Using Convolutional Neural Network to Improve Indonesian Government Cybersecurity." This study serves as a requirement for completing the Masters Program at the SoCS, Nusa Putra University. The successful completion of this final project was made possible due to the guidance, assistance, prayers, and cooperation of various parties.

The author realizes that the Final Project research this is still far from perfection, so the author expects criticism and suggestions from readers. I am hopeful that this research will contribute significantly towards creating a safer cyberspace by helping to classify and mitigate the threat posed by malware. As you delve into this thesis, I hope you find it informative, enlightening, and a useful contribution to the field of cybersecurity.

CHAPTER I
INTRODUCTION

1.1 Background

The rapid development of technology has a huge impact on daily life today. The development of technology is changing people's lifestyle very quickly, making them become more dependent on information technology, because it is considered to have the ability to facilitate all activities to be more efficient, productive and economical. It is now conceivably impossible to discern the real from the false with the naked eye due to the development of advanced Artificial Intelligence (AI) trained models utilized in the changes of digital information. The term "Deep fakes" has gained popularity in relation to these fake media materials. Deep fake techniques may be used to synthesize human images using artificial intelligence.

Deep fakes are the outcomes of using artificial intelligence to replace the voices and/or faces of persons in original photographs, video records, and audio recordings. Due to their numerous potential applications in deception, entertainment, and the propagation of false information, it has attracted a lot of interest. It uses artificial intelligence and machine learning techniques to create and modify audio and visual content that is used to disseminate misleading information. Deep learning and other artificial neural network techniques, including auto encoders or generative adversarial networks (GANs), are also used in the development of deep fake videos [1]. Deep fakes have been widely employed in recent years, necessitating the development of a system to identify them and reduce the amount of news that is fake or fabricated. It raises concern about this technology since processes have advanced to the point where it is difficult for people to discriminate between actual and false video information of faces [2]. Instantaneous photo and video capture and global transmission are also possible. Images and videos are frequently used by people to determine if an event actually took place. When "first-hand" accounts are recorded as videos, criminal and civil cases nowadays make headlines. These videos frequently spread across several platforms extremely fast. The lives of people involved are frequently left hanging in the balance due to this harmful dependence on these photographs and videos since the majority of the public trusts and believe what it sees and hears. A survey stated that Deep fake detection techniques encounter challenges such as limited datasets, unfamiliar media attack methods, temporal aggregation, and the presence of unlabeled data [3]. So that it needs a technology to maintain the issues. Machine Learning has accelerated the production of deep fake images and videos, making them faster and more cost-effective [4]. Although "deep fakes" carry a negative reputation, the technology is gaining traction in both commercial and individual settings. Recent technical progress has heightened the challenge of distinguishing between digitally manipulated images and authentic ones. The increasing prevalence of deep fake technologies has contributed to a growing sense of concern.

Conventional methods and approaches based on deep learning have been widely utilized. In contrast to conventional picture forensic methods, deep learning approaches integrate feature extraction and feature classification within a network structure, resulting in an end-to-end, efficient automatic feature learning classification methodology [5]. Deep learning methodologies in the context of video classifications offers detailed summaries of select studies and underscores the key insights derived from these investigations. The presentation of these key findings is intended to contribute to the research community's efforts in crafting novel deep learning models for video classifications [6]. It possesses the capability to identify deep fake videos in real-time, aiding in the prevention of misinformation dissemination and safeguarding our society. This holds significance in addressing and mitigating the adverse impacts associated with deep fake videos [7]. Research on deep fakes has widely carried out by researches, using the Long Short Term Memory (LSTM) method which provided good level accuracy and reliability in analyze any video and helps detecting deep fake face which have been manipulated, preventing people from deframing others [8]. A research presented a method that is sensitive to temporal aspects for automatically identifying deep fake videos. The proposed system utilizes a convolutional LSTM architecture for handling frame sequences. This experiments with a diverse collection of digitally modified videos showed that a basic convolutional LSTM structure could reliably predict whether a video had been manipulated, even with just 2 seconds of video data [9]. A previous study presented a video deepfake detection using CNN shows that the model decreased using low quality image and the accuracy needs to be furter increased with medium quality videos, that it needs combined models for a better training [10] while the other study presented that ResNext CNN-LSTM effectively identified deep-fakes in videos even in a small image size [11]. Other research about deep fake detection in video detection of digital media forensics results 91% of accuracy, LSTM method is proven to have a high level of accuracy in detecting a deep fake video [12]. A study combining CNN-LSTM and hand-crafted facial method while the results stated that CNN-LSTM give better perform than the hand-crafted facial method [13]. Whilst other research also conducted results 90% accuracy shown in deep fake video detection using CNN ResNeXt and LSTM [14]. Previous study also employed a deep learning (DL) method that integrated a long short-term memory (LSTM) network to analyze features extracted by a convolutional neural network (CNN). The primary innovation of this research was utilizing discrepancies in sequences and patterns of deepfakes for classification purposes [15].

According to previous research conducted, this research combined Long Short Term Memory (LSTM) and distributed computing method to detect the deep fake videos under the title "**Enhance Deep fake detection in videos using Long Short Term Memory with Distributed Computing".**

1.2 Problem Statement

With the rapid advancement of artificial intelligence and deep learning techniques, creating highly realistic deep fake videos has become easier and more cost-effective. This surge in the availability and sophistication of deep fake technologies has resulted in an increase in the dissemination of misleading information, making it increasingly difficult for individuals to distinguish between authentic and manipulated media. The potential for these manipulated videos to spread misinformation poses significant risks to societal trust in digital content, highlighting the urgent need for effective detection mechanisms.

Deep fake detection often lacks accuracy, leading to the potential spread of misinformation and the erosion of trust in digital content. To address this issue, we propose using Long Short Term Memory (LSTM) networks, which have shown promise in handling temporal data and can potentially improve the accuracy of deep fake detection systems.

Analyzing videos in real-time while maintaining high accuracy is a significant challenge. The combination of LSTM networks with distributed computing offers a promising solution to enhance deep fake detection. By leveraging LSTM's ability to analyze sequences of data and distributed computing's capacity to handle large-scale video processing efficiently, we aim to develop a more accurate and real-time deep fake detection system that can effectively combat the spread of manipulated media.

1.3 Research Objectives

1. To increase the accuracy and efficiency of deepfake video detection by combining LSTM and distributed computing approaches.
2. To Examine the performance of LSTM-based deep fake detection using distributed computing differ when applied to different number of deep fake cases.

3. To build and construct an efficient distributed computing system capable of improving the prediction of LSTM models for deepfake detection in real-time by using the capability of several computing units. The system should effectively distribute the computational workload, ensure data synchronization, and optimize resource utilization.

1.4 Significance of Study

The study of enhancing deepfake detection in videos using Long Short-Term Memory (LSTM) with distributed computing holds significant importance in the context of addressing the increasing concerns and potential threats posed by the proliferation of deepfake technology

1.5 Research Scope

The main scope of this study is to provide the insight combination of LSTM and distribute computing techniques improve the accuracy and efficiency of deep fake video detection compared to traditional detection methods. The combination of LSTM and distribute computing techniques was measured in different number of deep fake datasets to obtain the accuracy and efficiency of deep fake video detection compared to traditional detection methods.

1.6 Organization of Thesis

The rest of this thesis is organized as follows:

- Chapter I describes the background of problem that will be discussed in the thesis
- Chapter II describes the literature review of thesis
- Chapter III describes the methodology of thesis
- Chapter IV present the experiment result and discussion
- Chapter V conclusion the thesis and future work

CHAPTER V
CONCLUSION AND FUTURE WORK

5.1 Conclusion

In conclusion, the thesis titled "Enhance Deep Fake Detection in Videos Using Long Short Term Memory with Distributed Computing" represents a comprehensive exploration of cutting-edge technologies to bolster the capabilities of deep fake detection. The literature review provided a solid foundation by examining key concepts such as Deep Fake technology, ResNeXt_50 architecture, Artificial Intelligence, Neural Networks, Long Short-Term Memory (LSTM) networks, Distributed Computing, and the utilization of Confusion Matrix in the context of deep fake detection. The research methodology, characterized by functional requirements, meticulous data collection, feature extraction, LSTM modeling, and distributed computing, outlines a systematic and structured approach to address the challenges posed by sophisticated deep fake techniques. The experimental results and discussions emphasize the importance of each phase, ranging from data collection and preprocessing to analytics, evaluation, and prediction. The incorporation of distributed computing components like the Producer, Broker, and Worker nodes showcases the scalability and efficiency achieved in handling a multiple cases of deepfake videos.

The implementation of the deep fake detection system without distributed computing exhibited a significant processing time, taking approximately reducing the duration from 10.8 minutes to analyze a set of six deepfake video samples. This prolonged processing time can be attributed to the use of a single worker unit in the absence of distributed computing. However, upon integrating distributed computing into the deep fake detection system and leveraging three worker units, the testing duration for the same set of six deepfake samples was notably reduced from 10.8 minutes to 2.1 minutes, representing a 80.56% increase in speed. This enhancement in processing speed underscores the efficiency of the method in scaling up the detection process. The addition of multiple worker units through distributed computing proves instrumental in expediting the analysis of deepfake videos, making the system more adept at handling larger-scale dataset cases. This optimization can significantly contribute to the timely of deepfake video detection.

5.2 Future Work

In light of the notable advancements achieved in enhancing deep fake detection through the integration of Long Short Term Memory (LSTM) with Distributed Computing, there are several promising avenues for future research and development. Firstly, the scalability and efficiency demonstrated by the system highlight the potential for further optimization and refinement in distributed computing strategies. Exploring advanced parallel processing techniques and optimizing the allocation of computing resources could lead to even more significant reductions in processing time, particularly when dealing with larger and more complex datasets.

Additionally, future work could delve into the integration of real-time processing capabilities into the system. Developing mechanisms for on-the-fly analysis of streaming video content would be particularly valuable in the context of rapid and dynamic information dissemination on various online platforms. This could involve the exploration of edge computing solutions or the integration of real-time data processing frameworks to ensure timely detection and response to emerging deepfake threats .

Furthermore, considering the evolving nature of deepfake techniques, continuous research is needed to enhance the robustness of the detection model. This could involve the incorporation of more sophisticated features, continuous model training with updated datasets, and the exploration of ensemble learning techniques to improve overall detection accuracy.

REFERENCES

[1] Preeti, M. Kumar, and H. K. Sharma, “A GAN-Based Model of Deepfake Detection in Social Media,” *Procedia Comput. Sci.*, vol. 218, pp. 2153–2162, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.191.

[2] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Niessner, “FaceForensics++: Learning to Detect Manipulated Facial Images,” in *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019, pp. 1–11. doi: 10.1109/ICCV.2019.00009.

[3] A. Malik, M. Kuribayashi, S. M. Abdullahi, and A. N. Khan, “DeepFake Detection for Human Face Images and Videos: A Survey,” *IEEE Access*, vol. 10, pp. 18757–18775, 2022, doi: 10.1109/ACCESS.2022.3151186.

[4] U. Kosarkar, G. Sarkarkar, and S. Gedam, “Revealing and Classification of Deepfakes Video’s Images using a Customize Convolution Neural Network Model,” *Procedia Comput. Sci.*, vol. 218, pp. 2636–2652, 2022, doi: 10.1016/j.procs.2023.01.237.

[5] W. Zheng, X. Liu, X. Ni, L. Yin, and B. Yang, “Improving Visual Reasoning Through Semantic Representation,” *IEEE Access*, vol. 9, pp. 91476–91486, 2021, doi: 10.1109/ACCESS.2021.3074937.

[6] A. Rehman, S. B. Belhaouari, and A. Kabir, “Applied Sciences,” *Early Writings on India*, pp. 124–134, 2018, doi: 10.4324/9781315232140-14.

[7] Shilpa B, Anush Kamath, Anush Kamath, Hemanth Bhat, and Sathwik A M, “Unmasking Deepfakes: Using Resnext and LSTM to Detect Deepfake Videos,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 1, pp. 524–528, 2023, doi: 10.48175/ijarsct-8639.

[8] P. Yadav, I. Jaswal, J. Maravi, V. Choudhary, and G. Khanna, “DeepFake Detection using InceptionResNetV2 and LSTM,” *CEUR Workshop Proc.*, vol. 3058, pp. 1–6, 2021.

[9] D. Güera and E. J. Delp, “Deepfake Video Detection Using Recurrent Neural Networks,” in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 2018, pp. 1–6. doi: 10.1109/AVSS.2018.8639163.

[10] S. A. Aarti Karandikar, Vedita Deshpande, Sanjana Singh, Sayali Nagbhidkar, “Deepfake

Video Detection Using Convolutional Neural Network," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 4, no. 2, pp. 15–21, 2020, [Online]. Available: https://www.warse.org/IJATCSE/

[11] M. I. Abidin, I. Nurtanio, and A. Achmad, "Deepfake Detection in Videos Using Long Short-Term Memory and CNN ResNext," *Ilk. J. Ilm.*, vol. 14, no. 3, pp. 178–185, 2022, [Online]. Available: https://jurnal.fikom.umi.ac.id/index.php/ILKOM/article/view/1254

[12] V. Veera Venkata Naga Sai Vamsi, S. S. Shet, and S. Sai Mohan Reddy, "Deepfake detection in digital media forensics," *Glob. Transitions Proc.*, vol. 3, no. 1, pp. 74–79, 2022, doi: 10.1016/j.gltp.2022.04.017.

[13] S. Van Asseldonk, "Deepfake Video Detection using Deep Convolutional and Hand-Crafted Facial Features with Long Short-Term Memory Network," Tilburg University, 2021.

[14] D. Darwis, N. Siskawati, and Z. Abidin, "Penerapan Algoritma Naive Bayes Untuk Analisis Sentimen Review Data Twitter Bmkg Nasional," *J. Tekno Kompak*, vol. 15, no. 1, p. 131, 2021, doi: 10.33365/jtk.v15i1.744.

[15] Y. Doke, P. Dongare, V. Marathe, M. Gaikwad, and M. Gaikwad, "Deep Fake Video Detection Using Deep Learning," *Int. J. Res. Publ. Rev.*, vol. 3, no. 11, pp. 540–544, 2022, doi: 10.55248/gengpi.2023.4149.

[16] T. L. Wagner and A. Blewer, "'the Word Real Is No Longer Real': Deepfakes, Gender, and the Challenges of AI-Altered Video," *Open Inf. Sci.*, vol. 3, no. 1, pp. 32–46, 2019, doi: 10.1515/opis-2019-0003.

[17] X. Yang, Y. Li, H. Qi, and S. Lyu, "Exposing GAN-synthesized faces using landmark locations," *IH MMSec 2019 - Proc. ACM Work. Inf. Hiding Multimed. Secur.*, pp. 113–118, 2019, doi: 10.1145/3335203.3335724.

[18] A. Heidari, N. Jafari Navimipour, H. Dag, and M. Unal, "Deepfake detection using deep learning methods: A systematic and comprehensive review," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, no. August 2022, pp. 1–45, 2023, doi: 10.1002/widm.1520.

[19] P. Ghadekar, D. Khanwelkar, N. Soni, H. More, J. Rajani, and C. Vaswani, "A Semi-Supervised GAN Architecture for Video Classification," in *2023 International Conference on Advances in Intelligent Computing and Applications (AICAPS)*, 2023, pp.

1–7. doi: 10.1109/AICAPS57044.2023.10074051.

[20] O. Köpüklü, A. Gunduz, N. Kose, and G. Rigoll, "Real-time hand gesture detection and classification using convolutional neural networks," *Proc. - 14th IEEE Int. Conf. Autom. Face Gesture Recognition, FG 2019*, 2019, doi: 10.1109/FG.2019.8756576.

[21] R. Taviti, S. Taviti, P. A. Reddy, N. R. Sankar, T. Veneela, and P. B. Goud, "Detecting Deepfakes With ResNext and LSTM: An Enhanced Feature Extraction and Classification Framework," in *2023 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT)*, 2023, pp. 1–5. doi: 10.1109/IConSCEPT57958.2023.10170580.

[22] S. Jeevidha, S. Saraswathi, K. J. B, P. K, and N. Venkataramaya, "DEEP FAKE VIDEO DETECTION USING RES- NEXT CNN AND LSTM," vol. 11, no. 4, pp. 601–608, 2023.

[23] R. Cioffi, M. Travaglioni, G. Piscitelli, A. Petrillo, and F. De Felice, "Artificial intelligence and machine learning applications in smart production: Progress, trends, and directions," *Sustain.*, vol. 12, no. 2, 2020, doi: 10.3390/su12020492.

[24] P. Singh, C. Kumar, and A. Kumar, "Next-LSTM: a novel LSTM-based image captioning technique," *Int. J. Syst. Assur. Eng. Manag.*, vol. 14, no. 4, pp. 1492–1503, 2023, doi: 10.1007/s13198-023-01956-7.

[25] G. Van Houdt, C. Mosquera, and G. Nápoles, "A review on the long short-term memory model," *Artif. Intell. Rev.*, vol. 53, no. 8, pp. 5929–5955, 2020, doi: 10.1007/s10462-020-09838-1.

[26] J. Kang, S. Jang, S. Li, Y.-S. Jeong, and Y. Sung, "Long short-term memory-based Malware classification method for information security," *Comput. Electr. Eng.*, vol. 77, pp. 366–375, 2019, doi: https://doi.org/10.1016/j.compeleceng.2019.06.014.

[27] R. Buyya, C. Vecchiola, and S. T. Selvi, "Principles of Parallel and Distributed Computing," *Mastering Cloud Comput.*, pp. 29–70, 2013, doi: 10.1016/b978-0-12-411454-8.00002-4.

[28] L. A. Passos, D. Jodas, K. A. P. da Costa, L. A. S. Júnior, D. Colombo, and J. P. Papa, "A Review of Deep Learning-based Approaches for Deepfake Content Detection," 2022, [Online]. Available: http://arxiv.org/abs/2202.06095

[29] M. Jiwtode, A. Asati, S. Kamble, and L. Damahe, “Deepfake Video Detection using Neural Networks,” *2022 IEEE Int. Conf. Blockchain Distrib. Syst. Secur. ICBDS 2022*, 2022, doi: 10.1109/ICBDS53701.2022.9935984.

[30] Y. Al-Dhabi and S. Zhang, “Deepfake Video Detection by Combining Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN),” *IEEE Int. Conf. Comput. Sci. Artif. Intell. Electron. Eng. (CSAIEE), SC, USA*, pp. 236–241, 2021, doi: doi: 10.1109/CSAIEE54046.2021.9543264.

[31] P. Saikia, D. Dholaria, P. Yadav, V. Patel, and M. Roy, “A Hybrid CNN-LSTM model for Video Deepfake Detection by Leveraging Optical Flow Features,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2022-July, 2022, doi: 10.1109/IJCNN55064.2022.9892905.

[32] G. Wen, J. Qin, X. Fu, and W. Yu, “DLSTM: Distributed Long Short-Term Memory Neural Networks for the Internet of Things,” *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 111–120, 2022, doi: 10.1109/TNSE.2021.3054244.

[33] Z. Karimi, “Confusion Matrix,” no. October, pp. 260–260, 2021, doi: 10.1007/978-1-4899-7687-1_50.

[34] O. Caelen, “A Bayesian interpretation of the confusion matrix,” *Ann. Math. Artif. Intell.*, vol. 81, no. 3–4, pp. 429–450, 2017, doi: 10.1007/s10472-017-9564-8.

[35] L. S and K. Sooda, “DeepFake Detection Through Key Video Frame Extraction using GAN,” *2022 Int. Conf. Autom. Comput. Renew. Syst. (ICACRS), Pudukkottai, India*, pp. 859–863, 2022, doi: DOI: 10.1109/ICACRS55517.2022.10029095.

[36] A. Qadir, R. Mahum, M. A. El-Meligy, A. E. Ragab, A. AlSalman, and M. Awais, “An efficient deepfake video detection using robust deep learning,” *Heliyon*, vol. 10, no. 5, p. e25757, 2024, doi: 10.1016/j.heliyon.2024.e25757.

[37] S. Tanwar and J. Singh, “ResNext50 based convolution neural network-long short term memory model for plant disease classification,” *Multimed. Tools Appl.*, vol. 82, pp. 1–19, 2023, doi: 10.1007/s11042-023-14851-x.

[38] A. Gupta, P. Pawade, and R. Balakrishnan, “Deep Residual Network and Transfer Learning-based Person Re-Identification,” *Intell. Syst. with Appl.*, vol. 16, p. 200137, 2022, doi: https://doi.org/10.1016/j.iswa.2022.200137.

[39] M. Sangiorgio and F. Dercole, “Robustness of LSTM neural networks for multi-step

forecasting of chaotic time series," *Chaos, Solitons & Fractals*, vol. 139, p. 110045, 2020, doi: https://doi.org/10.1016/j.chaos.2020.110045.

[40] S. Yangui, A. Goscinski, K. Drira, Z. Tari, and D. Benslimane, "Future generation of service-oriented computing systems," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 252–256, 2021, doi: https://doi.org/10.1016/j.future.2021.01.019.

[41] Z. Xie, C. Ji, L. Xu, M. Xia, and H. Cao, "Towards an Optimized Distributed Message Queue System for AIoT Edge Computing: A Reinforcement Learning Approach.," *Sensors (Basel).*, vol. 23, no. 12, Jun. 2023, doi: 10.3390/s23125447.

[42] A. Ćatović, N. Buzađija, and S. Lemes, "Microservice development using RabbitMQ message broker," *Sci. Eng. Technol.*, vol. 2, no. 1, pp. 30–37, 2022, doi: 10.54327/set2022/v2.i1.19.