Foundation University Journal of Engineering and Applied Sciences

FUJEAS
Vol. 4, Issue 1, 2023.
DOI:10.33897/fujeas.v4i1.874

Research Article

Article Citation:
Shah et al. (2023). "Dynamic and Integrated Security Model in Inter Cloud for Image Classification". *Foundation University Journal of Engineering and Applied Sciences*
DOI:10.33897/fujeas.v4i1.874

Published by Foundation University Islamabad.
Web: https://fui.edu.pk/

Dynamic and Integrated Security Model in Inter Cloud for Image Classification

Ansar Munir Shah *, Itrat Abid

Department of Computer Science, Institute of Southern Punjab, Multan, Pakistan

* **Corresponding author**: amshah@isp.edu.pk

Abstract:

Cloud computing has transformed software and database accessibility, utilizing the Internet and server hosting. However, security risks arise, including malware attacks and website hacking. To address these challenges, deep learning models like ResNet50 have been developed. Trained on encrypted images, ResNet50 enhances the speed and accuracy of image recognition, enabling the identification of hidden data without decryption. Despite inter-cloud communication issues, cloud servers prioritize data security, user privacy, and integrity maintenance. The ResNet50 model exhibits impressive performance, achieving 99.5%accuracy and precision-recall scores of 99.5% and 99.5% using the ImageNet Dataset. Cloud computing offers significant advantages, but data security remains a critical concern. Encrypted image recognition powered by deep learning models offers efficient and private solutions. Cloud providers continually strive to improve inter-cloud communication, ensuring comprehensive protection for data and system integrity. The remarkable capabilities of ResNet50 highlight its potential in encrypted image analysis tasks.

Keywords: Infrastructure Management for Security; Deep Learning; Inter-Cloud; Image Encryption; ResNet50.

1. Introduction

The current cloud-based security model is predicated on the idea that the user or client can now have security in the cloud infrastructure. Businesses and individuals favor it because of its qualities of being affordable, scalable, and remotely accessible, however, there are huge problems in the cloud environment to address concerning data security, user privacy, and access control. Data belonging to a single user is directly ciphered using common encryption techniques including Identity-based cryptography Password based cryptographic protocols.

While the user's ID attributes are still not fixed and may change often, new features may be added, old attributes may be eliminated. Thus, a flexible feature control system is always required for real-time CP-ABE deployment. Due to their ability to store data across several servers and offer inter-cloud data transmission, multi-cloud storage systems significantly lower the risks associated with single-cloud storage systems [1].

1.1. Motivation

Due to their capacity to collect and understand low, mid, and high-level attributes from images, Concurrent Neural Networks (CNNs) is a go-to method for issues in the domain of computer vision and image analysis and have been widely applied in image recognition, object segmentation,

and other knowledge areas [2]. The intricacy of the CNN architecture is one of the main difficulties in deep learning-based surveillance. Image encryption, according to one definition, is the process of encrypting encrypted images using an encryption method so that only authenticated users may decrypt them [3]. Image encryption is crucial to ensuring the user's security and privacy and protecting against any unwanted authentication tokens. In many industries, image and video encryption is used in a variety of contexts, such as online communication, mobile applications, medical imaging, telemedicine, and military communication [4]. Transfer learning applied to data, and to increase the accuracy of the resNet50 model.

ResNet50 enhances the speed and accuracy of image recognition through several key mechanisms.

- Deep Residual Learning: ResNet50 presents the idea of residual learning, in which the model can learn residual functions by skipping one or more layers using shortcut connections. This makes it possible to train deeper models more successfully and lessens the degradation issue that particularly deep neural networks usually face.
- Skip Connections: ResNet50 allows data to move directly from early levels to later layers by utilizing skip connections. This makes it easier for gradients to propagate during training, which lessens the possibility of vanishing gradients and promotes model optimization.
- Bottleneck Architecture: ResNet50 uses a bottleneck architecture in its residual blocks to keep model depth while lowering computing costs.

This architecture maintains performance while increasing the speed of inference and training.

- Floating Point Operations, or FLOPs, are a measure of a model's computational complexity that is essential for evaluating the model's effectiveness, particularly in contexts with limited resources.
- Instruction and Interpretation Time: Two crucial variables, particularly for real-time applications, are the amount of time it takes to train the model on a given dataset and the amount of time it takes to produce predictions on newly discovered data**.**

1.2. Research Problems

The execution of such Inter-Cloud conditions isn't unimportant at all since Clouds are more convoluted than customary frameworks and the current interoperability and arrangement models are not material. There is the requirement for coordination of various security innovations, allowing a Cloud supplier to have the option to join the Inter Cloud without changing his security strategies or approval processes. Because of the elements of an Inter-Cloud united framework, an adaptable technique for building dynamic connections and empowering the conjunction of various and heterogeneous innovations ought to be given. The method will utilize the proposed model in the security of the board capabilities to be executed by the security of the executives' apparatuses. The use of firewalls and cryptography to fight assaults on IoT gadgets is contemplated to be the best approach to protection, however, because of the complications of IoT designs, this is not a viable option [5].

2. Literature Review

Authors [6] fostered the job of cloud security in big data Processing for cloud security systems and proposed the coordinated model in which Huffman coding is a strategy for correspondence information without forfeiting quality. An extensive variety of cloud security arrangements are accessible to help organizations decline chance and increment security. Cloud web security permits traffic to be coordinated to the cloud and utilizes AI calculation and encryption procedures. It is fundamental to make a framework that is both protected and quick to safeguard both oversaw and unmanaged enormous information [7].

Authors in [8] used encryption technique and cross-variety security methodology and the recommendations call for providing the encrypted message, a truly dumb idea. The use of electronic signatures puts the entire membership security at risk and could compromise other security measures a cryptographic hash estimate known as methods to danger capacity is employed in automated verification and all decent data of any kind. The organization behind the Cryptographic hash calculation is called N.I.S.T provides a 256-byte word if the length of the message is less than 264 parts message digest in a cycle. It is ensured that combining lopsided and symmetrical approaches will result in significant solid areas concerning safety they discovered that combining AES and RSA reduces the AES algorithm and overhauls speed.

Saxena et al. [9] proposed a framework in which VMs are dispensed utilizing First-Fit Decreasing calculation in light of the diminishing request of anticipated transmission capacity in order to lessen transfer speed wastage. To resolve this basic and testing issue, this letter recommends a cloud-based digital secure messaging model (OSC-MC) by recognizing and ending malignant VMs and between VM joins before the event of safety dangers. The atypical organization traffic, transmission capacity use, and unapproved between VM joins are security break pointers that direct asset allocation and secure cloud communication. The proposed model's recreation and comparison with already used approaches show that it essentially further develops approved between correspondence joins up to 34.5% with the decrease of organization resources, and power utilization by 66.46% and 39.31%, individually.

A three-layered model of cloud security confirmation identifies the top threats to the cloud This model and the proposed threat-showing technique will help professionals with organizing and increase trust in the cloud, implement a security confirmation architecture for a cloud environment, and hasten its absorption to gain agility and hasten the delivery of cloud services as well as apps in a useful way [10].

Budigiri et al. [11] proposed security requirements block their extensive gathering, especially in 5G URLLC edge applications with predominant execution and security necessities, since most security plans compromise execution. This makes finding a low above-compartment security game plan vital. For future work, it directs out the need to research the negative impedance between the Open stack network plan and the CNI-based network plan to decrease execution above of CNI module. the partner smaller than expected organizations should be sent on a comparative center point to ensure the best execution, which at any rate fabricates the prerequisite for the real withdrawal of different occupants.

Aldahwan et al. [5] utilized estimation air procedures and utilized cloud organization technique plans to carry out new groundwork on local area mists, with a specific accentuation on-request cloud expansions, which are regularly based on remote destinations for entomb cloud coordinated effort This paper played out a deliberate writing survey on local area cloud reception and the utilization of local area cloud advancements in different areas. Privately distributed computing frameworks can be incorporated thanks to the cloud-on-request method. Evenly to recognize utilized. Also, cloud planning calculation was utilized. There is an issue in deciding the variables influencing the reception of local area mists in advanced education foundations from a chief point of view.

Suhaas et al. [12] suggested the augmented network-aware and multi-parameter assistance-based robust communication method for inter-cloud networking environments in which he developed the optimization technique and by using deployment method inter-cloud networking environment was developed.

Havanje et al. [1] proposed the Intercloud Data Access Control Process: Dependable and Secure by using the ECDH (ECC+Diffie-Hellman) algorithm. Encryption technique was used in this proposed method. The AES algorithm was used in this method. All the encryption, decryption, and hash generation results are conducted with different file sizes on an average of 10 trials.

Sharma et al. [13] proposed resource discovery in an inter-cloud environment in which the proposed method was used and multiple techniques were applied. The paper presents some ideas to build effective and efficient resource discovery strategies for the inter-cloud.

Tripathy et al. [14] proposed the Oxidative and Protocol Integration: A Regional Internet Approach and robust operating system was obtained by ROS (Robot Operating System). It is a versatile solution because of loose coupling, late binding, and cyber security

Tejada et al. [15] proposed Enhancing Business Performance for Product Deliveries with a Cloud-Based Solution and an edges algorithm was used. That outcome clarifies how and where to deliver specific exported products to consumers supporting enterprise information system procedures with SAP and Azure Integration.

3. Proposed Model

3.2. Input Data

Data was given in encrypted images from Cloud 1 to Cloud 2, and communication was done through clouds.

3.3. Data Preprocessing

In order to train deep learning and its dependent models, image size is a challenge. All of the photos were standardized to ImageNet standards and downsized to 75 x 75 pixels, as part of the data pre-processing process. This was done because there are images of different sizes, and the size of the pictures interferes with the goal of giving high-level precision to identify the photographer's encrypted pictures and efficient retraining. Thus, the necessary steps to include it in our platform were to read all of the current image files.

To ensure comprehensive protection for data and system integrity in cloud environments, several measures can be taken:

- Encryption: To prevent unwanted access, data should be encrypted while it's in transit and at rest. While methods like disk encryption can secure data at rest, encryption protocols like SSL/TLS can be utilized for data in transit.
- Access Control: To limit access to critical information and resources, put strong access control measures in place. This covers least privilege principles, multi-factor authentication, and role-based access control (RBAC).
- Frequent Auditing and Monitoring: Track user activity, identify suspect behavior, and quickly address security events by utilizing logging, monitoring, and auditing tools. This contributes to maintaining the system's security and integrity.
- Use data redundancy and backup techniques to guard against losing data in the event of cyberattacks, hardware malfunctions, or accidents. This may entail frequent backups as well as data replication across several geographical sites.
- Security Awareness Training: To lessen the possibility of human error resulting in security breaches, teach staff members and users security best practices, such as selecting strong passwords, spotting phishing efforts, and adhering to correct data handling protocols.

3.4. Model Techniques

Firstly, used a combination of DES, Blowfish, and RC4 algorithms, writings written in Portuguese, English, and Spanish were encrypted. Data mining methods like J48, FT, PART, Addition Bayesian Network, and Multilayer Perceptron classifiers were applied to the encrypted files. Yet, there was still able to identify the technique utilizing data mining techniques Firstly Symmetric algorithm was used in which AES (Advanced Encryption Standard Algorithm) applied. It is faster than the Asymmetric algorithm but less secure. The proposed model is shown in Figure 1. Used the Asymmetric Encryption technique and RSA algorithm applied to secure the encrypted images. Because the asymmetric encryption technique is more secure and transfers large amounts of data.

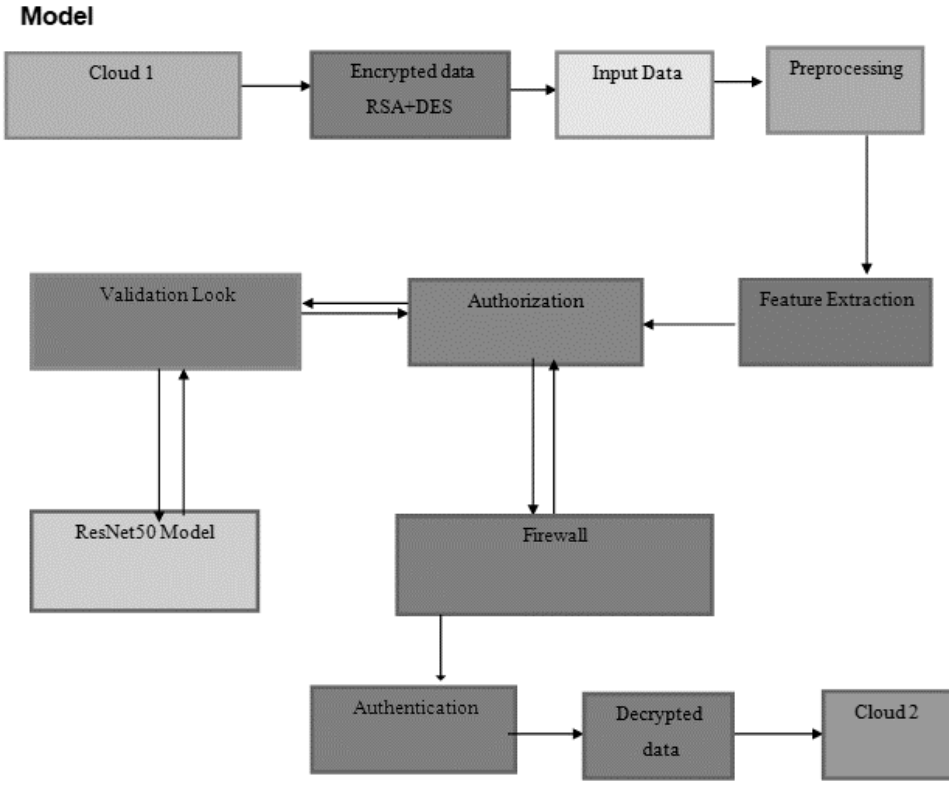

Figure 1: Proposed model

ResNet50 has been evaluated on various datasets, including but not limited to:

- ImageNet: An extensive dataset including more than 1.2 million photos of 1000 different types. Benchmarking the performance of image classification models, such as ResNet50, is frequently done using ImageNet.
- CIFAR-10 and CIFAR-100 datasets: 32x32 pixel photos from 10 and 100 classes are included in the CIFAR-10 and CIFAR-100 datasets, respectively. They are frequently employed to assess how well models perform in more manageable picture classification tasks.
- Homomorphic encryption (HE) is a technique used to train ResNet50 on encrypted images. With HE, encrypted data can be mathematically operated upon without needing to be decrypted. Generally, the procedure entails transforming picture data into an encryption-ready format, utilizing encryption techniques, honing the model using the encrypted data, and subsequently decrypting the model for deduction.
- ResNet50 uses a method known as secure multiparty computation (SMC), also known as federated learning, to handle feature extraction and classification in the context of encrypted picture input. In SMC, several parties work together to process their encrypted data in order to make calculations without disclosing the data itself. By running calculations on encrypted.

Similar to traditional image analysis, hyperparameters in ResNet50, like learning rate, batch size, and optimizer selection, have an impact on the model's performance in encrypted picture analysis shown in Figure 2.

3.5. Evaluation

Accuracy, recall, precision, and F1-score were the three evaluation metrics the proposed method employed in this study to assess how well the proposed classification model performed. They are defined by Equations (1), (2), (3), and (4), respectively. In accordance with statistical results from several tests, calculations are made.

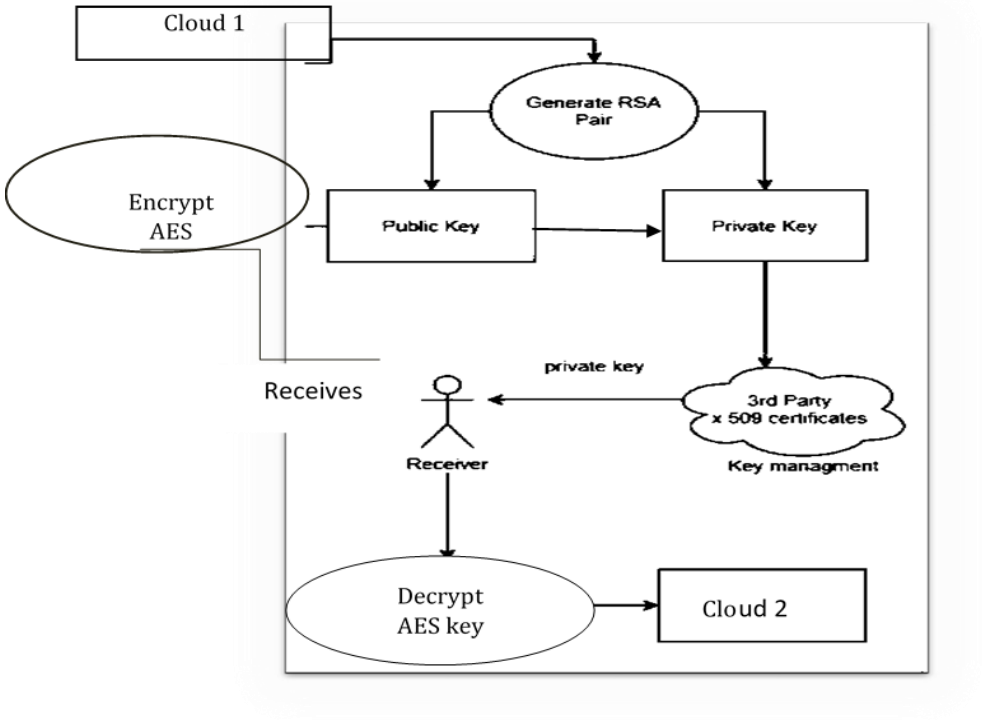

Figure 2: Encrypted data flow diagram in the proposed model

4. Results

The metrics that were utilized to evaluate the results of the deep mastering methods are compiled in this step. It is common practice to assess the effectiveness of gadget learning prediction algorithms and the outputs of the class set of rules. In this study, the accuracy of the device to assess the gadget and metrics like precision and taking into account confusion matrix were used to analyze the prediction findings. Prior to training the CNN classifiers using transfer learning, we detected Null values and scaled functions during the preprocessing stage The three proposed tactics had the desired results. We used, trained, and evaluated the Resnet50, CNN, and DCNN approaches. The Resnet50 set of rules, which had the greatest accuracy at 99.5%, was followed by the CNN which finished at 97.5%, even though reached 96% Prediction accuracy, and the findings suggested some improvement in image detection using these rules. CNN is currently superior to the other two models since it outperforms them in terms of accuracy and other performance metrics for the following reasons: First off, CNN is particularly adept at interpreting texts and the connections between the tokens, but Resnet50 can do well on image classification issues just as Resnet50 does for encrypted data in addition, CNN outperforms. Results and comparisons are shown in Tables 1 to 5 and Figures 3 to 4.

Table 1: Comparison of different algorithms

Method	No. of Classes	Accuracy	Precision	Recall	F1-score
Ref. [16]	10	96.70%	93.50%	91.95%	92.88%
Ref. [5]	10	95.80%	92.90%	93.75%	94.53%
Ref. [17]	10	95.91%	97.14%	98.82%	96.40%
Ref. [14]	10	97.75%	97.34%	96.52%	97.40%
Algorithm of this study	10	99.5%	99.5%	99.5%	99.5%

Table 2: Comparison of different algorithms

Evaluation Metric	Data (%)	Resnet50 (%)	CNN (%)
Accuracy	97	99.5	99.5
Precision	97	99.5	99.5
Recall	97	99.5	99.5

Table 3: Comparison of different algorithms

	Precision	Recall	F1-Score	Support
Class 0:	0.99	0.98	0.99	5063
Class 1:	0.98	0.99	0.99	4937
Micro Avg.	0.99	0.99	0.99	10000
Macro Avg.	0.99	0.99	0.99	10000
Weighted Avg.	0.99	0.99	0.99	10000

Table 4: Comparison of different algorithms

Layer (Type)	Output Shape	Param #
resnet50 (Model)	(None, 2048)	23587712
Dense (Dense)	(None, 2)	4098
Total params: 23,591,810 Trainable params: 4,098 Non-trainable params: 23,587,712		

Table 5: Comparison of different algorithms

Model	Year	Accuracy %	Precision %	Recall %	F1 Score %
CNN	2022	99.2	99.0	99.2	99.2
Resne50	2022	96.8	95.9	97.5	96.8
DCNN	2022	97.6	96.9	98.2	97.6
Our CNN Model	2023	99.5	99.5	99.5	99.5

Model accuracy is shown in Figure 3 and precision and recall comparison is shown in different models in Figure 4.

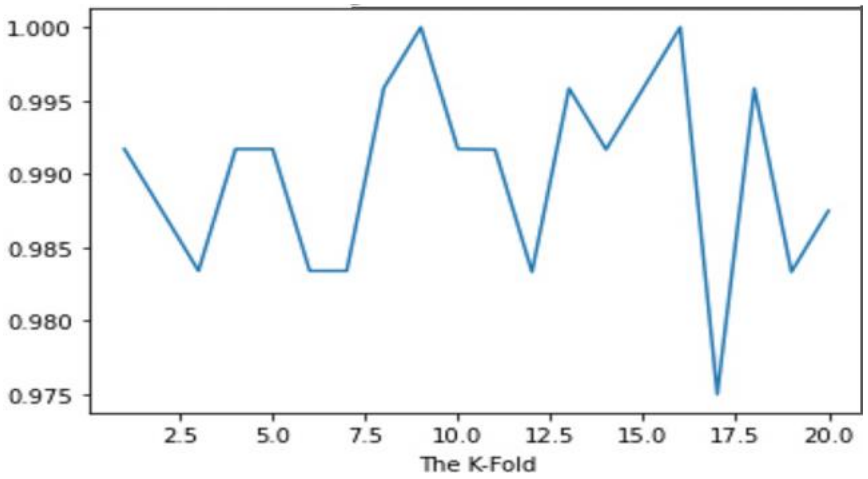

Figure 3. Model accuracy

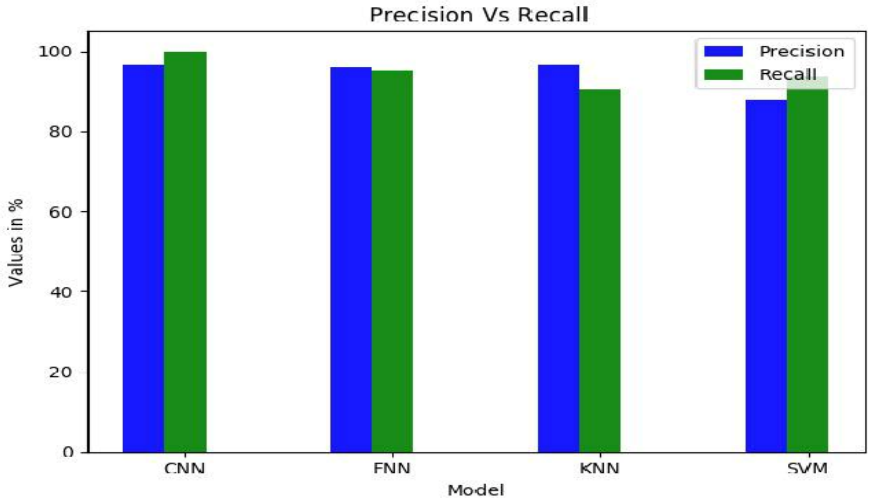

Figure 4: Precision vs recall accuracy

5. Conclusion

It's a difficult project to identify and explain inter-cloud security management concerns. To administrate Cloud services and applications, each public cloud deploys its own set of unique Cloud services and apps. As a result, cloud providers are unable to communicate with one another. Integration of diverse security systems is required. The proposed model will defend against attacks between inter-cloud communication and authorize the request and increase efficiency. In terms of the stated goals, the proposed model study succeeded in achieving by developing a model using deep learning that really can decode all these photos and correctly decrypt them. Using a pertained model for Keras, ResNet-50, with a dense model with softmax activation added on top and training with a reduced set of it was able to obtain a quite good model in terms of validation accuracy. The model was used to predict the classes of the images from the independent test set and results were submitted to test the accuracy of the prediction with fresh data.

6. Future Work

This proposed research can experiment with various systems to identify and analyze methods. Hyperparameters are tested for various deep-learning techniques. Additionally, to improve accuracy, the proposed model can employ deep learning, which mixes several machine learning algorithms in

accordance with some methodology (such as voting). Also, it will experiment with other encoding data encryption like DES and Blowfish.

Conflict of Interests

Publication of this research article has no conflict of interest.

7. References

[1] N. S. Havanje, K. R. A. Kumar, S. N. Shenoy, A. S. Rao and R. K. Thimmappayya, "Secure and reliable data access control mechanism in multi-cloud environment with inter-server communication security," *Suranaree Journal of Science & Technology*, vol. 29(3), 2022.

[2] S. Ahmad, S. Mehfuz and J. Beg, "Enhancing Security of Cloud Platform with Cloud Access Security Broker," In *Proceedings of Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, Springer, 2021, pp. 325–335.

[3] R. Dixit and K. Ravindranath, "Enhancement in Security for Intercloud Scenario with the Help of Role-Based Access Control Model," In *IOT with Smart Systems: Proceedings of ICTIS*, Springer Singapore, 2021, vol. 2, pp. 277–285.

[4] Z. Duliński, R. Stankiewicz, G. Rzym and P. Wydrych, "Dynamic traffic management for SD-WAN inter-cloud communication," *IEEE Journal on Selected Areas in Communications*, vol. 38(7), pp. 1335–1351, 2020.

[5] N. S. Aldahwan and M. S. Ramzan, "Descriptive Literature Review and Classification of Community Cloud Computing Research," *Scientific Programming*, pp.1–12, 2022.

[6] A. Shukla and N. Lodha, "Role Of Cloud Security in Big Data Processing for Healthcare System," In *8th International Conference on Advanced Computing and Communication Systems (ICACCS),* IEEE, 2022, vol. 1, pp. 61–67.

[7] W. Sirichotedumrong, Y. Kinoshita and H. Kiya, "Pixel-based image encryption without key management for privacy-preserving deep neural networks," IEEE Access, vol. 7, pp. 177844–177855, 2019.

[8] G. P. Kanna, A. Gupta, Y. Kumar and N. P. Patel, "An Enhanced Cloud-Based Healthcare System for Patient Data Privacy and Security Using Hybrid Encryption," In *2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, IEEE, 2022, vol. 2, pp. 112–117.

[9] D. Saxena and A. K. Singh, "OSC-MC: Online secure communication model for cloud environment," *IEEE Communications Letters*, vol. 25(9), pp. 2844–2848, 2021.

[10] R. Kumar and R. Goyal, "Top threats to cloud: a three-dimensional model of cloud security assurance," In *Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT*, Springer Singapore, 2020, pp. 683-705.

[11] G. Budigiri, C. Baumann, J. T. Mühlberg, E. Truyen and W. Joosen, "Network policies in kubernetes: Performance evaluation and security analysis," In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 407–412.

[12] K. P. Suhaas and S. Senthil, "A Robust Communication Strategy for Inter-Cloud Networking Environment through Augmented Network-Aware and Multiparameter Assistance," *Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases*, pp.159–173, 2022.

[13] M. Sharma, A. Gupta and J. Singh, "Resource discovery in inter-cloud environment: a review," *International Journal of Advanced Intelligence Paradigms*, vol. 23(1-2), pp.129–145, 2022.

[14] A. Tripathy, J. van Deventer, C. Paniagua J. Delsing, "Interoperability Between ROS and OPC UA: A Local Cloud-Based Approach," In *IEEE 5th International Conference on Industrial Cyber-Physical Systems*, IEEE, 2022, pp.1–5

[15] A. Tejada, K. Frolov and E. Overes, "On Cloud Solution to Improve Business Performance for Product Deliveries," In *Algorithms and Solutions Based on Computer Technology: 5th Scientific International Online Conference Algorithms and Solutions based on Computer Technology (ASBC 2021)*¸ Cham: Springer International Publishing, 2022, pp. 71-91.

[16] G. Wang, Y. Zhan, Y. Xia and L. Yan, "Distributed point-to-point routing method for tasks in cloud control systems," *Journal of Systems Engineering and Electronics*, vol. 33(4), pp. 792–804, 2022.

[17] H. Guo, W. Huang, J. Liu and Y. Wang, "Inter-Server Collaborative Federated Learning for Ultra-Dense Edge Computing," *IEEE Transactions on Wireless Communications*, vol. 21(7), pp. 5191–5203, doi: 10.1109/TWC.2021.3137843.