International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
Article Received: 04 December 2022 Revised: 30 December 2022 Accepted: 10 January 2023

Security Enhancement in Surveillance Cloud Using Machine Learning Techniques

[1.] Dr. Lingamallu Raghu Kumar, [2.] Dr. C. Ashokkumar, [3.] Dr. Purnendu Shekhar Pandey, [4.] Sathish Kumar Kannaiah, [5.] Balajee J, [6.] Dr. M. I. Thariq Hussan

[1]Assistant Professor
KG Reddy College of Engineering and Technology,
Department of Computer Science and Engineering,
Chilkur Village, Moinabad Mandal, RR district 501504
Telangana, India
lrgupta528@gmail.com
[2]Assistant Professor
Department of Computing Technologies,
School of Computing
SRM Institute of Science and Technology,
Kattankulathur, Chennai-603203
ashokkuc@srmist.edu.in
[3]Associate Professor,
Department of CSE,
KIET Group of Institutions,
Ghaziabad, U.P 201206
purnendu.pandey@kiet.edu
[4]Associate Professor,
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, Andhra Pradesh - 522502
ksathish1980@gmail.com
[5]Associate professor,
Department of Computer Science,
Mother Theresa Institute of Engineering and Technology,
Palamaner, Andhra Pradesh
j.balajee@mtieat.org
[6]Professor & Head
Department of Information Technology & CSE (IOT)
Guru Nanak Institutions Technical Campus
Ibrahimpatnam, Hyderabad – 501506, Telangana
thariqhussain@rediffmail.com

Abstract: Most industries are now switching from traditional modes to cloud environments and cloud-based services. It is essential to create a secure environment for the cloud space in order to provide consumers with a safe and protected environment for cloud-based transactions. Here, we discuss the suggested approaches for creating a reliable and safe environment for a surveillance cloud. When assessing the security of vital locations, surveillance data is crucial. We are implementing machine learning methods to improve cloud security to more precisely classify image pixels, we make use of Support Vector Machines (SVM) and Fuzzy C-means Clustering (FCM). We also extend the conventional two-tiered design by adding a third level, the CloudSec module, to lower the risk of potential disclosure of surveillance data.In our work we evaluates how well our proposed model (FCM-SVM) performed against contemporary models like ANN, KNN, SVD, and Naive Bayes. Comparing our model to other cutting-edge models, we found that it performed better, with an average accuracy of 94.4%.

Keywords: Image processing, machine learning, cloud computing, and surveillance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

I. Introduction

The Internet is utilised via a distributed computing method known as "cloud computing" to supply a variety of services (CC). The services could be provided as simple computer programmes designed to complete certain tasks, a platform for sharing online infrastructure, or any other platform made especially for the distribution of software over the Internet. Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service are the three categories that can be used to categorise cloud computing services in accordance with the definition above (SaaS). The standard cloud services have a few characteristics in common. A crucial element of cloud computing is service on demand, which enables the end-user to precisely specify how many resources are needed to fulfil their request. Applications, platforms, and infrastructures are allegedly made available through SaaS, PaaS, and IaaS services in response to consumer demand. The user's business data, which consists of personal information and business rules, are uploaded to all of the services. It is necessary to secure both personal data and business rules because doing so improves user satisfaction. Security must therefore be offered in SaaS, PaaS, and IaaS. The security level is very low not only in terms of services but also in terms of illegal users, access permissions, links or routes, data, and data storage. Another noteworthy feature of cloud computing is its high degree of elasticity, which gives businesses the freedom to adjust resource levels in response to demand and, as a result, significantly lowers costs. The fact that resources are not permanently linked to the user but rather are evaluated and taxed for usage at a very granular level while providing the cloud service is another crucial aspect of cloud computing. The cost incurred in acquiring static resources has been significantly reduced thanks to the pay per use model seen in cloud computing. Due to these features, various industries seem to be moving toward using cloud-based services. Figure 1 depicts the cloud computing architecture.

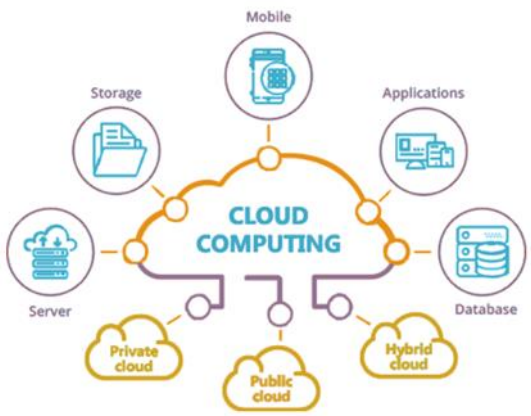

Figure 1. Cloud Computing Architecture

Public clouds like Microsoft Azure, Google Cloud Services, and Amazon Web Services are among the three basic types of cloud computing deployment methodologies (AWS), private clouds like Open Stack and VMWare that serve the needs of internal users, and hybrid clouds that blend public and private clouds. The public cloud environment is multitenant in nature when used, nevertheless, as a result of the fact that public-based cloud services serve a big population base. Information sharing is encouraged by the cloud environment's multitenant structure, which raises the danger of accessing the contents and data of other users. They are worried that commercially sensitive information won't be shared or will be compromised, many prestigious companies and industries are still hesitant to adopt cloud systems. The importance and necessity of cloud security as well as the need for complex and cutting-edge techniques to improve security in cloud systems have been further highlighted by this. A number of cloud-based data encryption standards and rules have recently been implemented in an effort to increase cloud security. Innovative identity detection, management, and tracking tools as well as a number of access management strategies have pushed for better security measures in cloud environments.

An AI-based system's decision-making capabilities are provided by machine learning (ML), one of the core subfields of artificial intelligence. [1]. Convolution neural networks (CNNs) are an advancement in machine learning that allow a system to learn how to make decisions by being trained with relevant data and being capable of handling varied circumstances. The primary advantages of machine learning are its speedy, human-free recognition of patterns and trends in the current flow. Continuous improvement is also a possibility when utilising machine learning techniques, particularly when the system is sensitive to shifting input. Machine learning has been employed in many applications that deal with multivariate and multidimensional data. Combining cloud computing with cutting-edge computing paradigms like artificial intelligence and machine learning has gained appeal as a way to finish various jobs and enhance cloud security. These research focus on using machine learning techniques and algorithms to improve cloud security.

Key Highlights

The key highlights of the proposed work are listed below:

i. The proposed model (FCM-SVM) combines the FCM and SVM ML approaches for higher levels of security enhancement.
ii. To lessen the risk of the potential disclosure of surveillance data, a Cloud Sec module was added to the traditional two-layered design.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

iii. The proposed FCM-SVM performed well, with a 94.4% average accuracy.

Organization of paper: This essay is divided into four sections: an introduction; a review of the literature; a methodology part for the suggested framework; and a conclusion. References are given at the end.

II. Related Works

Using ANN algorithms, Hussin et al. foresaw significant security challenges in distributed computing. Finding security holes in a banking institution required the deployment of an ANN algorithm. Algorithms from the Levenberg-Marquardt (LMBP) family were used to forecast the level of cloud security. To increase the brain's ability for learning and execution, ANNs were employed. The accuracy of the forecasts is evaluated using the mean square error (MSE), which is decided to decide the presentation, in order to narrow the gap between actual yields and the focus on preparation. Sayantan as well as others. It has been discovered that there are cloud characteristics that are essential for mitigating internet attacks on cloud settings. A trustworthy method was developed to detect digital intrusions on both cloud infrastructure and remote processing equipment. The suggested strategy calls for the use of ANN. The ANN was developed using system traffic information on the joining connections of cloud pauses. Because ANN is computationally comprehensive, a methodology that employs a hereditary computation to reduce the number of structures mined from the system-traffic information is built up and combined in this method.

An approach to classifying the data based on information confidentiality was proposed by Zardari et al. [70]. The writers offered a method for categorizing data that is subject to informational safety and protection. In virtual and cloud contexts, the K-NN knowledge architecture technique was applied. Data is grouped using K-NN with the goal of meeting security requirements. A DDoS detection method built on the C.4.5 algorithm was created by Zekri et al. [74] to minimize the threat of DDoS. Without previously making an account, individuals and organizations may now utilize programs and access their information on any PC with Web access thanks to CC. The results of the investigation suggest that C4.5 is the ideal grouping technique. The results of the DDoS detection test show that the detection accuracy is better than 98% and that the DDoS assault length exceeds the C4.5 algorithm's detection results. Many ML algorithms are employed to identify the DDoS threat. The C4.5 looks for the decision tree that is the shortest it can find.

Information security issues were covered by Grusho et al. [80] in their analysis of AI methods and models. The major sources of security threats for CC installations include the dynamic nature of CC systems, architectural obstacles prohibiting access to cloud infrastructure, and incorrect and illegal usage of cloud services computing. IDPs are employed to identify and stop information exchange participants who are breaking security rules, compile a list of the most recent dangers, and track them down. The various IDPS system types vary according to the particular events they should monitor and the methods they should employ. According to Hanna et al. [76], a decision tree (C4.5) technique is used for classification and data security. As a crucial first step toward acquiring a secure environment for distributed computing, they researched how to accomplish moderation for security concerns. The artwork in Table 1 is an example of contemporary work.

Table 1. State- of-art works

Authors	ML Method	Objective
Yuhong et al. (2015)	ANN	Public Cloud and private Cloud authorities
Grusho et al. (2017)	ANN	Privacy and security concerns employing ML for identification and clarity of information transfer
Park et al. (2018)	KNN	Privacy preserving
Calderon et al.	KNN+ Data Mining techniques	Reliable resource provisioning in joint edge Cloud environments
Wani et al.	SVM + Naïve Bayes	Intrusion detection
Arjunan et al.	Naïve Bayes	Intrusion detection
Chen et al.	SVD	User privacy
Feng et al.	SVD	Dimensionality reduction

III. Proposed methodology

The degree of data security afforded by off-site devices may actually vary depending on the cloud practitioners and service Amount Agreements selected. Particularly when it comes to a touchy subject like surveillance at strategic locations, cloud computing frequently makes privacy issues more challenging. In light of these circumstances, it is essential to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

offer rigorous anonymity protections for surveillance recordings in order to avoid internal or external parties from obtaining the personal data. The capacity of cloud service providers to process encrypted messages swiftly and surreptitiously is more important. We provide a novel technique in this respect to address privacy issues that arise while executing photograph analyzing distantly utilizing cloud computing. In seeking to address security concerns, our suggested cloud wonderful platform consists of two essential components, particularly system and privacy protection methodology.

Proposed System architecture

Consumer data is routinely exposed to various, serious security risks due to the typical cloud computing architecture. We provide a three-level architecture as a remedy for enhancing data security in a cloud environment. In our opinion, such a system comprises of three separate components: Client, CloudSec, and Cloud provider. In this paradigm, all surveillance data is initially encrypted via the HTTPS/SSL protocol by the CloudSec component. Second, segmentation is used in this module to protect surveillance photos. Data from clients is sent to an outside cloud provider for secure processing after being encrypted by CloudSec. This module is in charge of ensuring that client data is sufficiently private and secure when using cloud resources in this scenario. The suggested approach for dealing with security problems in cloud-based image processing is shown in broad strokes in Figure 2.

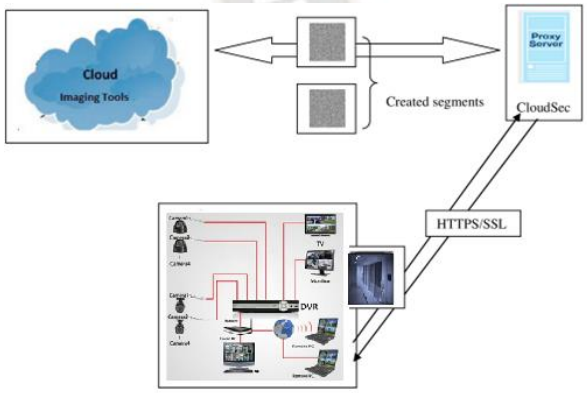

Figure 2. An Overview of cloud-based image processing

When accessing cloud resources in this situation, this module is in responsible of making sure that client data is appropriately private and safe. Figure 2 depicts in broad strokes the suggested strategy for addressing security challenges in cloud-based image processing. This latter module is incredibly strong, versatile, and useful for meeting security requirements in the cloud. The main strategy we utilise in our work to secure data is segmentation because it is an easy and efficient technique. The knowledge is effectively split into various groups in accordance with the attributes of the photographs, such as colour, texture, and shape, in order to achieve this using a particular method based on machine learning techniques.

Proposed Data protection Method

Although there are many uses for image segmentation algorithms that have proved effective, data protection is not one of those applications. Our main contribution is to apply this technique to cloud service security issues. In order to address each zone separately, it is intended to group pixels with comparable characteristics together. In this framework, in order to identify each pixel, From the input image, we first extract the colour at the pixel level. the classification Support Vector Machines with these features (SVM). Actually, the latter trains on real-world data using a supervised learning algorithm. To achieve this, we enhance the effectiveness of linear classification by training SVM Classifiers with Fuzzy C-means. Figure 3 depicts the fundamental concept of the SVM-based classification technique.

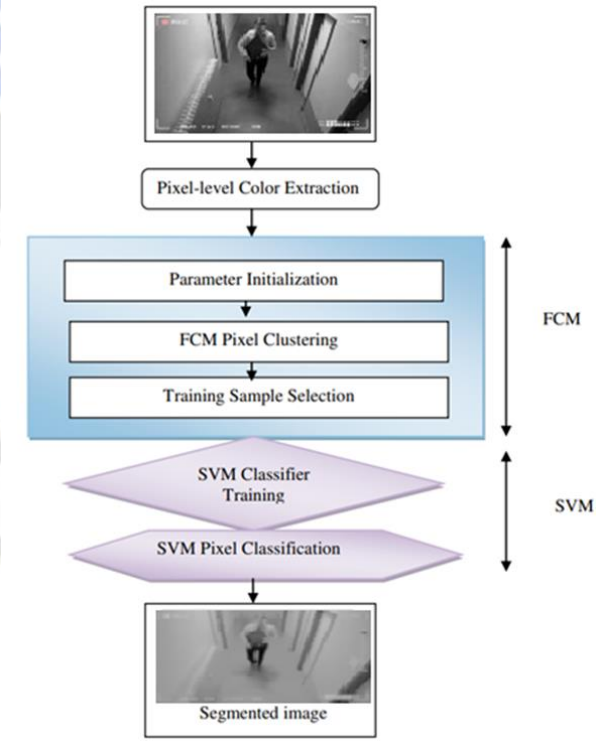

Figure 3. Proposed method for data protection

3.1 Used Methods

We demonstrate a novel support vector machine-fuzzy C-means clustering-based online privacy technique in this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
Article Received: 04 December 2022 Revised: 30 December 2022 Accepted: 10 January 2023

research. The main objective is to segment an image into discrete areas that include pixels with uniform image properties. The basic components utilised to portray an image are usually elements of colour, texture, and shape. Because of this, using FCM and SVM together is a good way to guard against the potential leak of sensitive information. This method, meantime, aims to deliver prompt and precise results. This section seeks to give comprehensive insight into the suggested approach.

- **Fuzzy C-means Clustering (FCM)**

The FCM method is an effective tool for unsupervised data processing and classification. The fuzzy technique allows each pixel to be a part of numerous clusters based on membership grades, in contrast to conventional partitioning methods (between 0 and 1). The main objective is to locate centroids that minimise the dissimilarity function. By initialising the membership matrix (U) arbitrarily, as shown in Equation 1, this can be accomplished quickly.

$$\sum u_{ij} = 1, \forall j = 1, \dots, n \quad \textbf{(1)}$$

Additionally, this approach classifies data using the dissimilarity function shown in Equation 2.

$$J\,(U, c_1, c_2, \dots, c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j=1}^{n} u_{ij}^m\, d_{ij}^2 \quad (2)$$

- The values of uij are normally between 0 and 1,
- ci stands for the centroid of the cluster I
- dij stands for the Euclidian distance between the ith centroid (ci)
- The jth data point, and m [1,] stands for a weighting exponent.

Support Vector Machines (SVM)

Machine learning techniques can be utilised to automate classification and regression using a straightforward yet effective method. Generalized linear classifiers are frequently employed in this strategy to analyse data and spot patterns. To achieve this, it primarily makes use of statistical learning theory. Actually, when dealing with a high dimensional feature space, we nearly always opt to use linear functions known as hypotheses. The main goals of SVM models are to maximise the smallest distance between any two data points and to discover the hyperplane that best divides various groups (margin). All locations on the margin are referred to as support vectors in this context. The simplest variation of this method, the linear SVM model, is shown in Figure 4 as a simplified illustration.

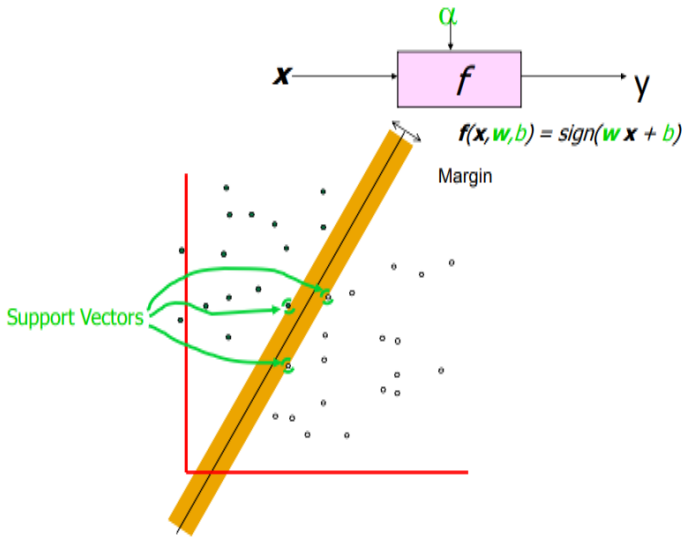

Figure 4. Linear SVM Model

To get the largest margin of separation possible in this scheme, we essentially use equation 3.

$$margin = \arg\min_{x \epsilon D} d(x)$$

$$= arg \min_{x \epsilon D} \frac{|x.w + b|}{\sqrt{\sum_{i=1}^{d} w_i^2}} \quad (3)$$

Where:

- Decision hyperplane normal vector is referred to as w.
- Reprents data point I is in xi.
- yi: represents the type of data point I (+1 or -1) NB: Not 1/0
- This formula is used to calculate the classifier: Sin(wT1 xi + b) = f(xi)
- The following formula represents the functional margin of xi: yi (wT1 xi + b)

Equation 4 represents a quadratic optimization problem that can be used to model hard-margin SVM mathematically.

$$\min_{f, \xi_i} \|f\|_k^2 + C \sum_{i=1}^{t} \xi_i$$

(4)

$$y_i f(x_i) \geq 1 - \xi_i \; for \; all \; i \; \xi_i \geq 0$$

Similar to the dual problem, equation 5 for learning linear classifiers is the simplest way to express the SVM.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

$$\min_{a_i} \sum_{i=1}^{1} a_i - \frac{1}{2} \sum_{i=1}^{1} \sum_{j=1}^{1} a_i\, a_j y_i y_j K(x_i, x_j) \qquad 0 \le a_i \le C, for\ all\ i;$$

$$\sum_{i=1}^{1} a_i y_i = 0 \qquad (5)$$

where I stands for slack variables, which are ideally utilised to represent measurement inaccuracy at a given moment (xi, yi).

Sincerity be damned, traditional means (hard margin) usually neglect data noise and uncertainties. To deal with noisy data, soft-margin SVM typically employs the idea of slack. The SVM formula changes to yi (w'x1 + b) 1 - Sk in this situation, where Sk is the shortest distance that can be used to separate data from the hyperplane without departing from the predetermined bounds. . These justifications convinced us to represent soft-margin SVM with the Lagrangian variable in equation 6.

$$\min L = {}^{1}/_{2}\, w'w - \sum \lambda_k(\lambda_k(w'^{x_k} + b) + s_k - 1) + a \sum s_k \qquad (6)$$

$$where, 0 \le a_i \le C\ for\ all\ a_i.$$

5. Performance Analysis

We used an 11th Gen Intel Core i5-11320H, Intel Iris Xe Graphics, 16 GB, 2 x 8 GB, DDR4, 3200 MHz, and 512 GB, M.2, PCIe NVMe, SSD to develop our suggested model (DCNN-FOA) in Pytorch. Several parameters, which are mentioned in table 2, were used to test our model.

True positive (TP): If your forecast is accurate and favourable;

True Negative (TN): If your forecast is accurate and favourable;

False Positive (FP): IF your prediction is both accurate and incorrect;

False Negative (FN): If your forecast is inaccurate and unfavourable

Table 2. Matrices of performance measures

	Performance Measures	Mathematical Equations
1.	Sensitivity, TPR	$\frac{TP1}{TP1 + FN}$
2.	Specificity, S	$\frac{TN1}{FP + TN1}$
3.	Precision	$\frac{TP1}{TP1 + FP}$
4.	Accuracy	$\frac{TP1 + TN1}{TP1 + FN + TP + TN1}$
5.	F Score	$\frac{2\,TP1}{2TP1 + FN + FP}$

Figure 5 shows the analysis of models with characteristics such as sensitivity, specificity, and accuracy of various datasets and average value. The comparison of models with respect to sensitivity, specificity, and accuracy is shown in Table 3. Figure 6 shows the corresponding graphs for the comparison of models with recall, f-score, and memory usage shown in Table 4. Figure 7 compares the suggested model to contemporary models.

Table 4. Comparison of models with sensitivity, specificity and accuracy

Dataset Sample	Models	Sensitivity (%)	Specificity (%)	Accuracy (%)
1	ANN	88	78	85.9
	KNN	87.3	84	87.4
	Naïve Bayes	89.6	88	90.3
	SVD	90.67	81	93.1
	FCM-SVM (ours)	91.2	89	94.4
2	ANN	83.9	82	80
	KNN	79.5	85	86.2
	Naïve Bayes	83	88.9	82.8
	SVD	85	80.3	87
	FCM-SVM (ours)	84	85	95
3	ANN	83.6	81	82.9
	KNN	82.9	84.5	86.5
	Naïve Bayes	86.6	86.3	84.5
	SVD	87.8	83.9	89.7
	FCM-SVM (ours)	88.4	88.3	94
4	ANN	87	77	84.8
	KNN	86.2	83	86.3
	Naïve Bayes	88.5	87	89.2
	SVD	89.56	80	92.01
	FCM-SVM (ours)	90.1	88	93.3

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

5	ANN KNN Naïve Bayes SVD FCM-SVM (ours)	89 88.4 90.7 91.77 92.3	79 85 89 82 90	86.1 88.5 91.4 94.2 95.55

Figure 5. Analysis of Models with parameters such as sensitivity, specificity and accuracy of various datasets and average value.

Table 5. Comparison of models with recall, f-score and memory utilization

Dataset	Models	Recall (%)	F-score (%)	Memory utilization (%)
1	ANN KNN Naïve Bayes SVD FCM-SVM (ours)	82 84.1 86.6 88 91	83.7 87 86 79 85	90 92 94 89 88
2	ANN KNN Naïve Bayes SVD FCM-SVM (ours)	83 85.2 87.3 89 92	84.8 88 87.1 80 86	91 93 95 90 89
3	ANN KNN Naïve Bayes SVD FCM-SVM (ours)	84 86.3 88.4 90 93	85.9 89 88.2 81 87	92 94 96 91 90
4	ANN KNN Naïve Bayes SVD FCM-SVM (ours)	82.10 84.2 86.7 88.1 91.1	83. 87.13 86.12 79.1 85.08	92.01 92.25 94.02 89.02 91.11
5	ANN KNN Naïve Bayes SVD FCM-SVM (ours)	84.02 86.5 88.6 90.04 93.5	86.12 89.25 88.5 81.2 87.20	92.20 94.02 96.6 91.01 90.02

Figure 6. Analysis of Models with parameters such as recall, F-score and Memory utilization of various datasets and average value.

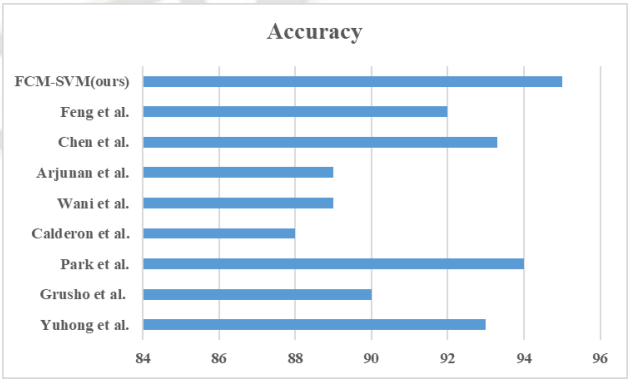

Figure 7. Comparison of models

IV. Conclusion

People view the cloud as a safer and more reliable method of data storage. Although data are more secure on the cloud,

malicious activities can still happen there. In delicate regions, like a surveillance network, it can have a strong reaction. We combined ML approaches to increase the security levels of the surveillance network. In this paper, an FCM-SVM technique for improving security in surveillance clouds is proposed. For lowering the risk of surveillance data, we added another Cloudsec module. Our proposed model performed well, with an average accuracy of 94.4%, when we compared it to other recent models like ANN, SVD, KNN, and Naive Bayes.

References

[1] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Security enhancement in healthcare cloud using machine learning." *Procedia Computer Science* 127 (2018): 388-397.

[2] Nassif, Ali Bou, Manar Abu Talib, Qassim Nasir, Halah Albadani, and Fatima Mohamad Dakalbab. "Machine learning for cloud security: a systematic review." *IEEE Access* 9 (2021): 20717-20735.

[3] Mohanty, Sachi Nandan, Gouse Baig Mohammad, Sirisha Potluri, P. Ramya, and P. Lavanya. "Next Generation Cloud Security: State of the Art Machine Learning Model." *Cloud Security: Techniques and Applications* 1 (2021): 125.

[4] Mohammad, Abdul Salam, and Manas Ranjan Pradhan. "Machine learning with big data analytics for cloud security." *Computers & Electrical Engineering* 96 (2021): 107527.

[5] Srikanth, N., and T. Prem Jacob. "An Real Time Cloud Security System and Issues comparison using Machine and Deep Learning." In *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 523-529. IEEE, 2021.

[6] Salman, Tara, Deval Bhamare, Aiman Erbad, Raj Jain, and Mohammed Samaka. "Machine learning for anomaly detection and categorization in multi-cloud environments." In *2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud)*, pp. 97-103. IEEE, 2017.

[7] Gupta, Ishu, Rishabh Gupta, Ashutosh Kumar Singh, and Rajkumar Buyya. "MLPAM: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment." *IEEE Systems Journal* 15, no. 3 (2020): 4248-4259.

[8] Ding, Aaron Yi. "Mec and cloud security." *Wiley 5G Ref: The Essential 5G Reference Online* (2019): 1-16.

[9] Karthika, P., and P. Vidhya Saraswathi. "IoT using machine learning security enhancement in video steganography allocation for Raspberry Pi." *Journal of Ambient Intelligence and Humanized Computing* 12, no. 6 (2021): 5835-5844.

[10] Tiwari, Chandra Shekhar, and Vijay Kumar Jha. "Enhancing Security of Medical Image Data in the Cloud Using Machine Learning Technique." *International Journal of Image, Graphics and Signal Processing* (2022): 13-31.

[11] Mohanta, Bhabendu Kumar, Debasish Jena, Utkalika Satapathy, and Srikanta Patnaik. "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology." *Internet of Things* 11 (2020): 100227.

[12] Cohen, Aviad, and Nir Nissim. "Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory." *Expert Systems with Applications* 102 (2018): 158-178.

[13] Xiao, Liang, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." *IEEE Signal Processing Magazine* 35, no. 5 (2018): 41-49.

[14] Schelter, Sebastian, Felix Biessmann, Tim Januschowski, David Salinas, Stephan Seufert, and Gyuri Szarvas. "On challenges in machine learning model management." (2015).

[15] Chiba, Zouhair, Noreddine Abghour, Khalid Moussaid, and Mohamed Rida. "Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms." *computers & security* 86 (2019): 291-317.

[16] Aldallal, Ammar, and Faisal Alisa. "Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning." *Symmetry* 13, no. 12 (2021): 2306.

[17] Panker, Tomer, and Nir Nissim. "Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux

[18] Qureshi, Basit, and Anis Koubâa. "Five traits of performance enhancement using cloud robotics: A survey." *Procedia Computer Science* 37 (2014): 220-227.cloud environments." *Knowledge-Based Systems* 226 (2021): 107095.

[19] Natarajan, Jayapandian. "Cyber secure man-in-the-middle attack intrusion detection using machine learning algorithms." In *AI and Big Data's Potential for Disruptive Innovation*, pp. 291-316. IGI global, 2020.

[20] Mishra, Narendra, R. K. Singh, and Sumit Kumar Yadav. "Design a New Protocol for Vulnerability Detection in Cloud Computing Security Improvement." In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*. 2021.

[21] Sangui, Smarta, and Swarup Kr Ghosh. "Cloud Security Using Honeypot Network and Blockchain: A Review." *Machine Learning Techniques and Analytics for Cloud Security* (2021): 213-237.

[22] Rath, Mamata, and Sushruta Mishra. "Advanced-level security in network and real-time applications using machine learning approaches." In *Research Anthology on Machine Learning Techniques, Methods, and Applications*, pp. 664-680. IGI Global, 2022.

[23] Quraishi, Suhail Javed. "Machine Learning Approach for Cloud Computing Security." In *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 158-163. IEEE, 2022.

[24] Tiwari, Pradeep Kumar, K. Kannan, Duggineni Veeraiah, Nikhil Ranjan, Jain Singh, Ghalib H. Alshammri, and Awal Halifa. "Security Protection Mechanism in Cloud Computing Authorization Model Using Machine Learning Techniques." *Wireless Communications and Mobile Computing* 2022 (2022).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

[25] Hema, C., and Fausto Pedro Garcia Marquez. "Storage Enhancement in the Cloud Using Machine Learning Technique and Novel Hash Algorithm for Cloud Data Security." In *International Conference on Management Science and Engineering Management*, pp. 516-526. Springer, Cham, 2022.

[26] Alrashdi, Ibrahim, Ali Alqazzaz, Esam Aloufi, Raed Alharthi, Mohamed Zohdy, and Hua Ming. "Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning." In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0305-0310. IEEE, 2019.

[27] Uppal, Mudita, Deepali Gupta, Sapna Juneja, Adel Sulaiman, Khairan Rajab, Adel Rajab, M. A. Elmagzoub, and Asadullah Shaikh. "Cloud-Based Fault Prediction for Real-Time Monitoring of Sensor Data in Hospital Environment Using Machine Learning." *Sustainability* 14, no. 18 (2022): 11667.

[28] Thenappan, S., M. Valan Rajkumar, and P. S. Manoharan. "Predicting diabetes mellitus using modified support vector machine with cloud security." *IETE Journal of Research* (2020): 1-11.

[29] Ali, Elmustafa Sayed, Mohammad Kamrul Hasan, Rosilah Hassan, Rashid A. Saeed, Mona Bakri Hassan, Shayla Islam, Nazmus Shaker Nafi, and Savitri Bevinakoppa. "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications." *Security and Communication Networks* 2021 (2021).

[30] Vora, Utsav, Jayleena Mahato, Hrishav Dasgupta, Anand Kumar, and Swarup Kr Ghosh. "Machine Learning–Based Security in Cloud Database—A Survey." *Machine Learning Techniques and Analytics for Cloud Security* (2021): 239-269.

[31] Mondal, Avijit, and Radha Tamal Goswami. "Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security." *Microprocessors and Microsystems* 81 (2021): 103719.

[32] Mondal, Avijit, and Radha Tamal Goswami. "Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security." *Microprocessors and Microsystems* 81 (2021): 103719.

[33] Muddala, Saikrishna, and Charanya Ramakrishnan. "Review of Face Recognition Techniques for Secured Cloud Data Surveillance using Machine Learning." In *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, pp. 1-10. IEEE, 2020.

[34] Zekri, Marwane, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. "DDoS attack detection using machine learning techniques in cloud computing environments." In *2017 3rd international conference of cloud computing technologies and applications (CloudTech)*, pp. 1-7. IEEE, 2017.

[35] Chkirbene, Zina, Aiman Erbad, Ridha Hamila, Ala Gouissem, Amr Mohamed, and Mounir Hamdi. "Machine learning based cloud computing anomalies detection." *IEEE Network* 34, no. 6 (2020): 178-183.

[36] Alshammari, Amirah, and Abdulaziz Aldribi. "Apply machine learning techniques to detect malicious network traffic in cloud computing." *Journal of Big Data* 8, no. 1 (2021): 1-24.

[37] Reddy, SaiSindhuTheja, and Gopal K. Shyam. "A machine learning based attack detection and mitigation using a secure SaaS framework." *Journal of King Saud University-Computer and Information Sciences* (2020).

[38] Diener, Michael, Leopold Blessing, and Nina Rappel. "Tackling the cloud adoption dilemma-A user centric concept to control cloud migration processes by using machine learning technologies." In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 776-785. IEEE, 2016.

[39] Rath, Mamata, Jyotirmaya Satpathy, and George S. Oreku. "Artificial intelligence and machine learning applications in cloud computing and internet of things." In *Artificial intelligence to solve pervasive internet of things issues*, pp. 103-123. Academic Press, 2021.

[40] Sharma, Abhishek, and Umesh Kumar Singh. "Modelling of Smart Risk Assessment Approach for Cloud Computing Environment using AI & supervised machine learning algorithms." *Global Transitions Proceedings* (2022).

[41] Kumar, Yogesh, Surabhi Kaul, and Yu-Chen Hu. "Machine learning for energy-resource allocation, workflow scheduling and live migration in cloud computing: State-of-the-art survey." *Sustainable Computing: Informatics and Systems* 36 (2022): 100780.

[42] Kannagi, A., J. Gori Mohammed, S. Sabari Giri Murugan, and M. Varsha. "Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbor algorithm for cloud security applications." *Materials Today: Proceedings* (2021).

[43] Wallis, Kevin, Christoph Reich, Blesson Varghese, and Christian Schindelhauer. "QUDOS: quorum-based cloud-edge distributed DNNs for security enhanced industry 4.0." In *Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing*, pp. 1-10. 2021.

[44] Kishor, Amit, Chinmay Chakraborty, and Wilson Jeberson. "A novel fog computing approach for minimization of latency in healthcare using machine learning." (2021).

[45] Sharkh, Mohamed Abu, Yong Xu, and Eric Leyder. "CloudMach: cloud computing application performance improvement through machine learning." In *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1-6. IEEE, 2020.

[46] Sasirekha, S. P., N. Mohanasudaram, P. Sherubha, and V. Manikandan. "An Enhanced Vehicle to Cloud Communication by Prediction Based Machine Learning Approaches." In *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, pp. 1-4. IEEE, 2020.

[47] Tahsien, Syeda Manjia, Hadis Karimipour, and Petros Spachos. "Machine learning based solutions for security of Internet of Things (IoT): A survey." *Journal of Network and Computer Applications* 161 (2020): 102630.

[48] Pop, Daniel. "Machine learning and cloud computing: Survey of distributed and saas solutions." *arXiv preprint arXiv:1603.08767* (2016).

[49] Pop, Daniel. "Machine learning and cloud computing: Survey of distributed and saas solutions." *arXiv preprint arXiv:1603.08767* (2016).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6154
***Article Received**: 04 December 2022 **Revised**: 30 December 2022 **Accepted**: 10 January 2023*

[50] Renugadevi, G., B. Raj Kumar, A. Karthikeyan, and E. Iohn Prince. "Improvement of health efficiency using cloud and machine learning." In *AIP Conference Proceedings*, vol. 2519, no. 1, p. 030074. AIP Publishing LLC, 2022.

[51] Kale, Rahul Vishwanath, Bharadwaj Veeravalli, and Xiaoli Wang. "A Practicable Machine Learning Solution for Security-Cognizant Data Placement on Cloud Platforms." In *Handbook of computer networks and cyber security*, pp. 111-131. Springer, Cham, 2020.

[52] Saran, Munish, Rajan Kumar Yadav, and Upendra Nath Tripathi. "Machine Learning based Security for Cloud Computing: A Survey." *International Journal of Applied Engineering Research* 17, no. 4 (2022): 332-337.

[53] Hesamifard, Ehsan, Hassan Takabi, Mehdi Ghasemi, and Catherine Jones. "Privacy-preserving machine learning in cloud." In *Proceedings of the 2017 on cloud computing security workshop*, pp. 39-43. 2017.

[54] Miao, Yinbin, Wei Zheng, Xiaohua Jia, Ximeng Liu, Kim-Kwang Raymond Choo, and Robert Deng. "Ranked Keyword Search over Encrypted Cloud Data Through Machine Learning Method." *IEEE Transactions on Services Computing* (2022).

[55] Alzahrani, Ahmed Saeed. "An optimized approach-based machine learning to mitigate DDoS attack in cloud computing." *International Journal of Engineering Research and Technology* 13, no. 6 (2020): 1441-1447.

[56] Yadav, Saumya, Rakesh Chandra Joshi, and Divakar Yadav. "Trustworthy Machine Learning for Cloud-Based Internet of Things (IoT)." In *Transforming Management with AI, Big-Data, and IoT*, pp. 155-167. Springer, Cham, 2022.

[57] Almuzaini, Khalid K., Amit Kumar Sinhal, Raju Ranjan, Vikas Goel, Rajeev Shrivastava, and Awal Halifa. "Key Aggregation Cryptosystem and Double Encryption Method for Cloud-Based Intelligent Machine Learning Techniques-Based Health Monitoring Systems." *Computational Intelligence and Neuroscience* 2022 (2022).

[58] Saran, Munish, Rajan Kumar Yadav, and Upendra Nath Tripathi. "Machine Learning based Security for Cloud Computing: A Survey." *International Journal of Applied Engineering Research* 17, no. 4 (2022): 338-344.

[59] Angelopoulos, Angelos, Emmanouel T. Michailidis, Nikolaos Nomikos, Panagiotis Trakadas, Antonis Hatziefremidis, Stamatis Voliotis, and Theodore Zahariadis. "Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects." *Sensors* 20, no. 1 (2019): 109.

[60] Muthulakshmia, K., and K. Valarmathib. "Attaining Cloud Security Solution Over Machine Learning Techniques." *Smart Intelligent Computing and Communication Technology* 38 (2021): 246.

[61] Kaur, Prableen, Manik Sharma, and Mamta Mittal. "Big data and machine learning based secure healthcare framework." *Procedia computer science* 132 (2018): 1049-1059.

[62] Rajput, Deepak Singh, Saurabh Sharma, Shiv Kumar Tiwari, A. K. Upadhyay, and Ashish Mishra. "Medical data security using blockchain and machine learning in cloud computing." In *Mathematical Modeling and Soft Computing in Epidemiology*, pp. 347-374. CRC Press, 2020.

[63] Hesamifard, Ehsan, Hassan Takabi, Mehdi Ghasemi, and Rebecca N. Wright. "Privacy-preserving machine learning as a service." *Proc. Priv. Enhancing Technol.* 2018, no. 3 (2018): 123-142.

[64] Potluri, Sirisha, Katta Subba Rao, and Sachi Nandan Mohanty, eds. *Cloud Security: Techniques and Applications*. Vol. 1. Walter de Gruyter GmbH & Co KG, 2021.

[65] Rajarajeswari, P., M. Sreevani, and P. Lalitha Suryakumari. "Secure Cloud Risk Architecture analysis for Mobile Banking system and its performance analysis based on Machine learning approaches." In *Journal of Physics: Conference Series*, vol. 2089, no. 1, p. 012007. IOP Publishing, 2021.