KARPAGAM JCS

www.karpagampublications.com

Volume : 20 **Issue : 01** **Jan - Feb 2025**

CONTENTS **PAGE No.**

1. **SECURITY ESTABLISHMENT IN INTERNET OF THINGS TO MANAGE TRAFFIC USING INTEGRATED LEARNING APPROACHES** 1
S.Nanadhini, S.Thilagavathi

2. **A SURVEY ON PREDICTING AND CONTROLLING AIR POLLUTION USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES** 8
Ninsha V Unnikrishnan, S Mythili

3. **A STUDY ON DERMATOLOGICAL DIAGNOSIS OF CARDIOVASCULAR DISEASE THROUGH MULTIMODAL FUSION OF ARTIFICIAL INTELLIGENCE** 13
J. Albert Irudaya Raj, K. Lakshmi Priya

4. **IoT BASED SECURE TRANSACTION IN REMOTE PATIENT MONITORING USING CRYPTOGRAPHY TECHNIQUES** 18
C.Preethika, E.J.Thomson Fredrik

5. **MACHINE LEARNING FOR INTRUSION DETECTION: TRENDS, CHALLENGES AND FUTURE DIRECTIONS** 26
Resmi Krishnan V, S. Mythili

6. **END-TO-END DEEP CONVOLUTIONAL PRINTED ID FACIAL IMAGE STEGANOGRAPHY TO PREVENT FROM PHOTOGRAPH SUBSTITUTION ATTACK** 35
Kiruthika N, Nandhini GS

SECURITY ESTABLISHMENT IN INTERNET OF THINGS TO MANAGE TRAFFIC USING INTEGRATED LEARNING APPROACHES

*S.Nanadhini** [1], *Thilagavathi* [2]

ABSTRACT

The Internet of Things (IoT) has seen an extraordinary growth rate recently; meanwhile, cybercrime activities have also gained unwanted attention, posing security threats. This is proved by the number of communication media and IoT devices being attacked by cybercrime. The IoT users will face severe losses in finances and service interruption when the attacks are not quickly detected and rectified. Cyber-attacks will impose an identity protection threat. Real-time intrusion detection is essential to make services based on the Internet of Things reliable, profitable and secure. This study projects a contemporary system for intrusion detection in IoT devices based on deep learning (DL). This paper introduces an intelligent system with deep network architecture to identify the malicious traffic that might attack IoT devices. To decrease the complexities in deployment, The proposed Deep Learning-based Intrusion Detection (DLID)-based Xtreme Gradient Boosting (XGB) system has been built as a model independent of the communication protocol. During the analysis of the proposed system's performance, reliable outcome is achieved in both real-time and simulated environments. Our model's accuracy of 94.75% on average is completed by detecting anomalies such as distributed DoS, black hole detection, wormhole attacks, sinkholes, and opportunity services. Precision value of 94.71%, F1-score of 94.82% and recall value of 95.47% is achieved on average by the system proposed for intrusion detection. IDS systems based on innovative deep learning provide an average detection rate of 93.2%, considered acceptable for IoT network security.

Keywords: IoT, network security, machine learning, deep leanring, prediction

Department of Computer Science and engineering[1],
Karpagam Academy of Higher Education, Coimbatore, India[1]
nandhini.sivaraj@kahedu.edu.in
NGM College, Pollachi[2]
thilagavathibluesky@gmail.com
* Corresponding Author

I. INTRODUCTION

This computing system brings about a new shift in people's lives called The Internet of Things (IoT). In a vast number of applications, IoT devices are used. A few of these applications are as follows: healthcare, smart homes, including transportation, supply-chain management [1], industrial production, Blockchain monitoring and security. The author have carried out research which states that by 2025, devices connected to IoT will reach a whooping number of 30.9 billion. A previous study says that 13.8 billion [2] IoT devices were present in 2021. This shows that this industry achieves 55% of the growth rate. So, because of its rapid growth, the business potential has attracted the attention of corporate people, researchers, devices dependent on IoT, innovators, entrepreneurs, business people, and lastly, cyber-criminals [3]. In the market, there is a high demand for the services provided by devices connected to IoT. So, potential investors are showing great interest in this new field. To make people's lives so much easier, entrepreneurs and innovators are developing various attractive and promising services based on IoT devices. However, the same interest for a better life has enabled criminals to attack vulnerable, weak devices connected to IoT cyber-attacks with fewer security features. Cyber-attackers are taking this opportunity to practice their malicious activities in attractive domains like finance and business. This is the primary reason for the growing number of attacks on devices connected to IoT [4].

The security of IoT devices is studied by [5], who express that when manufacturing IoT devices, very little attention is paid to cybersecurity or even no attention is paid. Research conducted and proposes that many IoT devices present in the field currently in different services are fully operational but are vulnerable to attacks from cyber criminals [6]. Attacks are not confined to IoT devices. Devices with IoT service are not stand-alone devices. They are connected to various other systems and appliances, which makes them an attack vector, allowing the attackers to exploit the devices connected to

them by gaining their access. In 2016, primary internet-dependent services like Netflix, Amazon and Twitter faced devastating effects of internet outages due to imaging IoT devices connected through Dyn coming under the cyber-attack [7]. Medical IoT, or MioT, is the fastest-rising sector based on IoT service usage. Since healthcare is a sensitive field and needs strict privacy, an attack on MIoTs will be devastating. The trends in cyber-attacks in recent times show that the MIoT device intrusion rate is higher than ever, and it is snowballing at a high pace.

Security vulnerabilities in IoT devices are the primary shortcoming faced by the Internet society. IoT devices with vulnerabilities can be exploited more ways than we think [8]. Systems connected to IoT devices are constrained computationally. Other than cyber-physical attacks (out of the scope of this research), every other cyber-attack is made possible using network connectivity, which is not within this scope. It is impractical to secure vulnerable IoT environments using conventional methods for cyber-security.

Furthermore, there are several ways the vulnerabilities of IoT devices can be exploited, so the traditional or rule-based security methodology needs to fit the security requirements of today's internet world. Vast volumes of data are constantly produced in IoT environments. It is challenging to detect anomalous data from the sea of legitimate data. In cases like these, approaches based on Deep Learning (DL) are appropriate. Analyzing and classifying massive data, discovering patterns among them, and finding relations based on the properties defined are challenging tasks, and deep neural networks are highly capable of doing this analysis. Hence, it is used in our proposed system.

In IoT security and intrusion detection based on anomaly, a promising security solution is provided using Deep Neural Networks (DNN) applications. Even though the IoT environment tends to produce large volumes of data, a similar pattern is formed by data due to its shared nature. Any data that does not follow the natural pattern will be considered abnormal. A network that is adequately trained can be a potential solution for identifying and classifying anomalous data [9]. A system for detecting intuition from real-time anomalous data in an IoT environment based on a proposed model with the help of the hypothesis provided above. This research is being put forward to build an independent IoT intrusion detection system with a communication protocol through a deep neural network to provide a secure and safe IoT environment.

In this research, we proposed a (DLID) Deep Intrusion-Detection system, a IDS. The main advantage of this system is that it does not need network structure virtualization, system attributes or any communication protocol modification. When DLID is connected to a network, it will detect the standard data flow and anomalous signal flow. Intrusions are detected by finding the data flow signals that deviate from the consistent signal pattern. This paper provides the following core contributions:

- ❖ Design and optimization of DLID-based Xtreme Gradient Boosting for intrusion detection in a network connected to an IoT environment.
- ❖ Structuring of components embedded in the system for intrusion detection.
- ❖ They are identifying excellent features for datasets to train the IoT network to detect intrusion effectively.
- ❖ An intrusion model with commonly occurring attacks of five numbers was used for the DLID-based intrusion detection system's thorough analysis.
- ❖ An average rate of 94.7% intrusion detection is achieved in a network.

The work is organized as: section 2 describes the literature work. The methodology is provided in section 3. The numerical results are given in section 4 and conclusion in section 5.

II. RELATED WORKS

IoT devices and their services have made our day-to-day lives so much easier. Most of the sectors and their access have been revolutionized by their application. Even though IoT devices achieve a remarkable growth rate, their adoption by people from all industries could be better due to cybersecurity concerns. It poses a significant barrier to the adoption pace of IoT technologies. When an IoT device is attacked successfully, other devices connected to it will be

prone to be explored by cyber-criminals, so it causes a cascading effect on the devices connected to IoT. At the application level, IoT devices are extensively used; they are commonly used to make human personal aspects easier. This is one of the primary reasons cyber-criminals target attacks on IoT devices [11].

Furthermore, big manufacturing units control the units' activities through IoT device automation. If a breach in security is to happen, then the whole system and its access will be in the hands of the attacker. During situations like this, a harmless smartphone or watch connected to IoT will become vulnerable to such unwarranted attacks. These features make cybercriminals interested in attempting to attack extensive facilities connected to IoT. In order to reduce the number of cyber-attacks on IoT devices, we should develop an intrusion detection system based on Deep Learning.

In their review paper, the author proposed different methods and their effectiveness in detecting and eliminating intrusions in IoT environments. The authors exhibit an excellent performance rate for detecting intrusion in IoT network built the SHAP model by using a deep learning technique. They employed the network's Shapley additive explanations (SHAP) and exhibited improved results. The primary feature of this system is that the Deep Learning-based IDS's decision-making is analyzed logically to understand the working principle. The SHAP framework exhibits a promising 99.15% and 98.83% accuracy and F1 score, respectively. The field of interest for the SHAP framework is (IoV) Internet of Vehicles. It is an IoT sub-branch. The author in [12] stated that intrusion detection systems based on ML work exceptionally in environments like edge and fog computing. The proposed intrusion detection system works optimally for any IoT network without constraints to the connected devices. In the meantime, an accuracy of 99.15% is attained by A. Oseni et al., which brings some doubt about excessive data, and it has to be tested with various datasets with diverse data to address the suspicion. Our system is more robust and reliable when the above framework is compared with the proposed IDS.

A deep Learning-based system named DeepIIoT was established. It intends to provide proper security to IoT devices connected to the industry; it succeeded in its mission by exhibiting an accuracy of 99% when executed with the collected testing dataset. Their area of interest is primarily power grids, facilities for water treatment, and nuclear reactors based on heavy industrial IoT devices. A dataset named WUSTL-IIOT-2021 is employed for training and testing the framework [13]. The deep learning-based IDS is proposed to cover all IoT devices and to provide better security at every level. However, network-independent IoT service is provided by the novel intermediate communication system. Unlike other sector-specific applications, the IDS system and its application offer services for various sectors. Furthermore, the DeepIIoT system is a detection system based on a rule and depends on the signature for processing. One of the challenges faced is recurrent updating, which is needed for every database use. There are no such barriers in the system we proposed. In the framework presented by V. Ravi et al., an ensemble meta-classifier is employed in the intelligent network intrusion detection system they developed; it uses a fusion approach with recurrent deep learning features. The framework mentioned above exhibits an average accuracy of 99% [14]. Even though the above method provides a higher accuracy rate, its network architecture is complex and challenging to deploy, whereas the proposed method overtakes simple network architecture. So, it gives a fresh perspective on the IoT domain and its future enhancements. The author presented a methodology for intrusion detection using mining-based ANN. Intrusion detection in communication networks demonstrates substantial improvement. ANNs are employed in the proposed approach. However, network architecture is particularly premeditated for identifying IDS in IoT networks. Meaning it is domain-specific.

DL techniques in IoT security is expressed in IoT privacy can also use this application and its uses in future work, as they emphasized [15]. Developing rule-based intrusion detection systems specific to certain networks is easy because they will perform well only within the particular network. H G. An et al. developed a sinkhole attack intrusion detection system, a knowledge-based network dependent on

a specific rule. This system provides an 81.63% attack detection ratio, which is 7% better performance than; an approach named INTI is presented. An open course networks for rule-based intrusion detection systems and their variations in dynamic analysis, discussed the importance of using suitable IDS for different configurations and networks [15]. The motto of the methodology proposed and the above paper's quantitative analysis fall perfectly together; this is needed for intrusion detection systems in a network applied with IoT, independent of the protocol used.

III. METHODOLOGY

3.1. Dataset

For this experiment, 25,000 instances were arranged, which constitutes one dataset. In the provided dataset, 82:18 is the instance ratio of Regular (R_D) to Malicious (M_D). It can be explained as, out of 25,000 instances, malicious data accounts for 18% and regular data accounts for 82%. In the prepared dataset, no pattern was formed intentionally, and M_D. and R_D are mixed randomly. In the ratio of 70:15:15, the data in the dataset were separated into training, testing, and validation data. During the training phase, the validation and training datasets have been utilized. Only during the phase of experimental evaluation is the testing dataset put into use; it is kept undisturbed during the validation and training phase. In systems for automatic intrusion detection, it is essential to perform appropriate feature reduction and feature selection for enhanced detection. So, for this experiment, An ML algorithm-based intrusion detection system determines the influential features for better outcomes.

3.2. Method

The DLID system proposed and represented in Fig 1. This is an automatic system with cutting-edge capabilities. The DLID learned the host IoT network and the data they generated, and the intrusion was detected as soon as it received sufficient training. The proposed IDS's dynamic connector will initiate the link between the emulated network, and the IoT network is asked for the request fulfilment. Using an interface module, the network classifier and feature extractor will communicate in the simulated network. The network packet's features are extracted through a feature extractor used as the proposed deep neural network dataset. With the help of the classifier Updater module, the recently identified features are updated regularly. That's why the IDS system proposed is said to be dynamic. Whenever an intrusion is found to have happened, the network classifier will pass it to mitigation stage. So, reducing the intrusion impact of this phase. Quantitative and qualitative features are presented. Receivers and senders will be in the network connected to IoT. Devices connected to IoT are designed to communicate in the least complex way possible because these devices are constrained to use resources. The receiver's and senders' transmission rates are kept the same to eliminate the need to install the extended buffer memory. DoS attack can be defined as a substantial variation in the distribution and transmission rate.

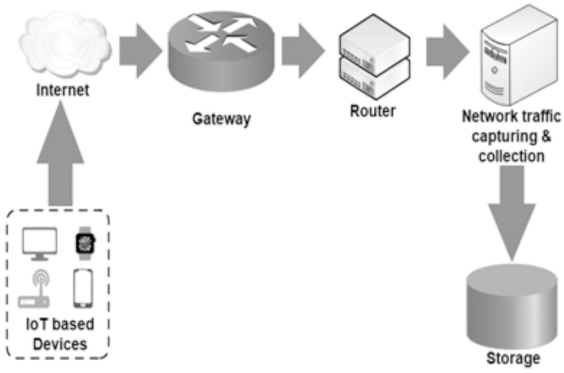

Figure 1 : Umbalanced network traffic

IoT network is safe when the reception and transmission ratio is near unity. Moreover, the ratio deviates substantially from unity. In that case, it indicates that the receiver is not getting data from intended source and the sender is not transferring it to the intended source. This indicates spoofing. There are some unlisted intermediate devices by which the security has been breached, and an external source manipulates the receiver and the sender. The communication protocol determines the communication cycle status, the following phase, and the transmission mode. A DLID is trained to communicate under various transmission modes. When some device behaves unfamiliarly in a particular transmission mode, the network is found to have intruded. In

an IoT network, qualitative results will be the outcome of quantitative analysis, which will help the system confirm intrusion in an IoT device. Quantitative analysis uses the features presented to produce qualitative results. If a device is under attack, the DLID will use the Communication Module's cache memory to store these features temporarily. It will use them to spot the possible intrusion successfully. This is done by calculating the probability distribution with the help of the following Eq. (1).

$$P_d = P(f_0), P(f_1), P(f_2), \dots, P(f_7) \quad (1)$$

Here is Eq. (1), $P(f_i)$ specifies probability of every data packet identified in i^{th} feature. If the mean of the $P(f_i)$ is above 50%, then the data is malignant/benign.

ML-based algorithm uses gradient-boosted model to boost performance and speed. Compared to other gradient-boosting methods, XGB shows outstanding speed. The blend of earlier models' ideas was used to form the new models to achieve ultimate outcomes. The proposed model's performance will be improved, and loss will be brought down by employing this gradient descent method. When ML-based problems are analyzed, the above process is appreciated by data scientists as it provides an end-to-end tree-boosting technique. Two primary components are embedded within XGB: regularization and training loss, θ denoting the ideal training data " and XGBoost.

$$O(\theta) = L(\theta) + \Omega \quad (2)$$

Here, the training loss function is represented by L , the metric used to evaluate model's performance in predicting the training samples. Mean Squared Error (MSE) is represented as a training loss function:

$$L(\theta) = \sum_i (y_i - \hat{y}_i)^2 \quad (3)$$

In logistic regression, the frequently employed loss function is the logistic loss function:

$$L(\theta) = \sum_i [y_i \ln(1 + e^{-\hat{y}_i}) + (1 - y_i) \ln(1 + e^{-\hat{y}_i}) \quad (4)$$

The regularization process controls the model's complexity; this factor helps by eliminating the overfitting issue, and it is given as follows:

$$\Omega(f) = \gamma T + \frac{1}{2} \lambda \sum_{j=1}^{T} ||w||^2 \quad (5)$$

IV. NUMERICAL RESULTS

This study uses Python with the TensorFlow library to implement the proposed DLID system for IoT networks. Cooja Network Simulator (CNS) is employed here. The Contiki Operating System (COS) is used for experimentation. The introduced intrusion detection system's experimentation and performance were evaluated using metrics derived from cutting-edge ML techniques. The researchers found that precision, accuracy, F1-score, and recall are the evaluation metrics broadly employed based on ML. Eq. (6) to Eq. (10) define these metrics in the order of accuracy, recall and F1-score. False Negative (FN), True Negative (TN), False Positive (FP) and True Positive (TP) are used to measure the evaluation metrics. The confusion matrix analysis present in the following subsection contains these values. The proposed DLID system's intrusion Detection Rate (IDR) performance is evaluated, and Equation (17) presents the same. Here, Detected Intrusion is given as DI, and Total Intrusion is given as TI.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

$$Precision = \frac{TP}{TP + FP} \quad (7)$$

$$Recall = \frac{TP}{TP + FN} \quad (8)$$

$$F1 - score = 2 * \frac{precision * recall}{precision + recall} \quad (9)$$

$$IDR = \frac{DI}{TI} * 100\% \quad (10)$$

Table 1 lists overall performance based on intrusion type. The DLID system's comprehensive performance analysis is done by experimenting with random attacks in a live environment. Owing to confidentiality and security issues, we DLID not allow unknown attackers to exploit our system by opening it. Nevertheless, the DLID system's performance is evaluated using a realistic intrusion model; for this experimentation, our system is monitored round the clock (24h). Many random attacks happened during this time. Detected intrusions were thus made and logged for evaluation and record.

Table 1 Performance comparison

Attack	Acc	Pre	Re	F1	IDR
Blackhole	94	94.6	96.1	94.2	98.5
DoS	94.9	94.8	95.3	94.6	95.4
OS	96.2	96.1	96.3	95	91
Sink hole	94	94.3	94.2	93.8	92.8
Worm hole	95.6	95.6	94.5	94.3	92.3
Average	**94.7**	**94.7**	**93.8**	**94.4**	**93.2**

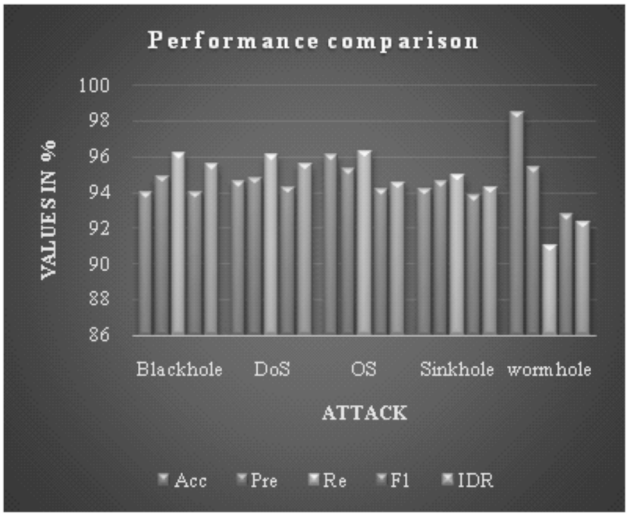

Figure 2 : Performance comparison

Fig. 2 demonstrates the system's overall performance. The deep learning-based IDS has exhibited the best outcome in identifying (OSA) Opportunistic Service Attacks. Yet, it does not mean that DLID needs to perform better in other systems. The proposed system for all intrusion detection exhibits 94.74% accuracy on average, 94.172% precision, 95.824% recall, and 95.472% F1 score. For all five attack types, the intrusion detection rate is observed. DLID protects against most experimenting attacks, and 95.11% of the average IDS is kept. Fig 2 illustrates that borderline variation is observed in average accuracy, precision, recall, and F1-score. Evaluation metrics' average value range is 94% to 95%, presented in yellow. This indicates that the DLID system detects intrusion automatically in practical applications on IoT networks in a stable, suitable and accurate way, hence better protecting the network's devices.

V. CONCLUSION

With the present boom in the IoT sector, smart devices connected to IoT communicate with one another and themselves to perform required tasks. This scenario is backed by the 30.9 billion active IoT devices. The vast 65% development in the IoT sector makes business people, entrepreneurs, educationalists, and cybercriminals gravitate towards IoT. Owing to the computing environment's resource-constrained feature, IoT device manufacturers need to pay attention to security while concentrating on quality of service. Attacks made on IoT do not end on the same device but will move to all other devices connected to it, jeopardizing the entire network. That is why it attracts cybercriminals more than ever in the internet-dependent environment. This influenced us to develop a system for intrusion detection as soon as attackers make an attempt, which we found to be much more essential. The novel deep learning-based IDS detects frequent and commonly attempted attacks with 94.74% average accuracy. A deep learning-based based DLID-XGB is trained for a specific network performs fine over the heterogeneous environment. The proposed system collects datasets from various from different networks. This novel method is a fresh wave of air for IoT device security as it provides a scalable and robust intrusion detection system and automatically detects intrusion; it also can learn from other IoT networks. A platform-independent framework that can be developed for IoT networks from the DL-based IDS will be explored for future scope. It is anticipated that a proposed framework's lightweight version will be much more effective and efficient in detecting intrusion.

REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015.

[2] Reddy, Y. Ramadevi, and K. V. N. Sunitha, "Effective discriminant function for intrusion detection using SVM," in Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICAC), Sep. 2016, pp. 1148–1153.

[3] Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," in Proc. Int. Conf. Signal Process. Commun. Eng. Syst., Jan. 2015, pp. 92–96.

[4] Farnaaz and M. A. Jabbar, "Random forest modelling for network intrusion detection system," Procedia Comput. Sci., vol. 89, pp. 213–217, Jan. 2016.

[5] Khan and N. Jain, "A survey on intrusion detection systems and classification techniques," Int. J. Sci. Res. Sci., Eng. Technol., vol. 2, no. 5, pp. 202–208, 2016

[6] Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software-defined networking," Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), Oct. 2016, pp. 258–263.

[7] Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness based semi-supervised learning approach for an intrusion detection system," Inf. Sci., vol. 378, pp. 484–497, Feb. 2017.

[8] Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness based semi-supervised learning approach for an intrusion detection system," Inf. Sci., vol. 378, pp. 484–497, Feb. 20

[9] Chang, W. Li, and Z. Yang, "Network intrusion detection based on random forest and support vector machine," Proc. IEEE Int. Conf. Comput. Sci. Eng./IEEE Int. Conf. Embedded Ubiquitous Comput., Jul. 2017, pp. 635–638

[10] Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016. [Online]. Available: http://arxiv.org/abs/1612.07640

[11] Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P.-A. Manzagol, "Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion," J. Mach. Learn. Res., vol. 11, pp. 3371–3408, 2010.

[12] In Proc, you, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning-based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016, pp. 225–229.

[13] Sherubha, "Graph Based Event Measurement for Analyzing Distributed Anomalies in Sensor Networks", Sådhanå(Springer), 45:212, https://doi.org/10.1007/s12046-020-01451-w

[14] Sherubha, "An Efficient Network Threat Detection and Classification Method using ANP-MVPS Algorithm in Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-11, September 2019

[15] Sherubha, "An Efficient Intrusion Detection and Authentication Mechanism for Detecting Clone Attack in Wireless Sensor Networks", Journal of Advanced Research in Dynamical and Control Systems (JARDCS), Volume 11, issue 5, Pg No. 55-68

A SURVEY ON PREDICTING AND CONTROLLING AIR POLLUTION USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES

*Ninsha V Unnikrishnan** [1], *S Mythili* [2]

ABSTRACT

Since air pollution has a significant negative influence on public health, early warning systems must be able to make precise long-term predictions about air quality. Predicting air quality has garnered a lot of interest, combining computer science, statistics, and environmental science. The Paper reviews a number of studies on air pollution, its effects on mental health, and the use of machine learning methods for air quality monitoring and prediction. Some of the studies investigate the connection between mental health outcomes and air pollution. They draw attention to the substantial influence that air pollutants, especially PM2.5, have on mental health conditions like depression and psychotic episodes. Machine learning techniques are used in many research to forecast pollution levels and air quality. To predict air quality indicators and particular pollutant concentrations, this research uses a variety of models, including Support Vector Machines (SVM), Random Forests, Neural Networks, and ensemble techniques like XGBoost. Innovative methods of environmental monitoring, such as the application of AI, IoT, and computer vision technologies, are the subject of certain studies. These technologies are used in urban settings to identify and categorize different types of pollution, including visual pollution. The combined findings of these studies highlight the substantial harm that air pollution causes to the general public, especially to mental health, and show how cutting-edge technologies can be used to monitor, forecast, and control air quality in metropolitan settings.

Department of Computer Science[1]
Karpagam Academy of Higher Education, Coimbatore, India[1]
ninshavu@gmail.com[1]
Department of Computer Science[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
smythili78@gmail.com[2]

* Corresponding Author

Keywords: Air pollution; Machine learning; Neural Network; Random Forest; XGBoost

I. INTRODUCTION

Air pollution is a serious environmental problem that has an effect on public health since it causes heart disease, respiratory illnesses, and even mental health issues. Effective monitoring and forecasting of air quality has become increasingly important as urbanization and industrial activity continue to increase. Researchers are looking into cutting-edge technology because traditional approaches to air pollution monitoring frequently have issues with accuracy and scalability. In this area, machine learning has become a potent instrument, providing data-driven methods for predicting air quality, analyzing pollution trends, and creating early warning systems. Machine learning helps to reduce the detrimental impacts of air pollution on public health by combining computer science, statistics, and environmental science to enable more accurate and timely responses.

Accurate long-term air quality forecasts are crucial given the pressing need for efficient monitoring and mitigating measures. Machine learning approaches are being used to predict and monitor air quality as a result of recent developments in computer science, statistics, and environmental science. This study examines a number of research that investigate the connection between mental health and air pollution, as well as the use of cutting-edge technologies like artificial intelligence (AI), the Internet of Things (IoT), and computer vision in the evaluation of air quality.

II. LITERATURE SURVEY

(i) Prediction of air pollution using Machine Learning.

In [1], the study focuses on employing a multi-task learning (MTL) framework to forecast hourly pollutant concentrations (such as SO_2, PM 2.5, and ozone) employing,

PM2.5, and ozone) employing cutting-edge regularization techniques (such as the 2,1-norm, nuclear norm, and Frobenius norm) to improve forecast stability and accuracy. By predicting several time steps at once, it highlights temporal dependencies. On the other hand, in case of [2] the authors uses Support Vector Regression (SVR) to forecast pollutant levels and the Air Quality Index (AQI), with an emphasis on classification accuracy. Because of its capacity to represent nonlinear environmental data, the Radial Basis Function (RBF) kernel was used. [1] performs better than traditional regression models, with a focus on higher generalization and parameter reduction whereas [2] uses unseen validation to show 94.1% classification accuracy for AQI prediction

In order to support public health and urban planning, [3] is mainly focusing on predicting Tehran's PM2.5 and PM10 levels. It highlights the necessity of precise air pollution prediction models. Whereas [9] Focuses mostly on PM2.5 pollution and its effects on health, especially in emerging and heavily populated areas, emphasizing emissions from traffic and industry.

In [3] the authors make use of a variety of machine learning models, such as artificial neural networks (ANN), geo-weighted regression (GWR), support vector machines (SVM), and autoregressive nonlinear neural networks (ARNN). Also presents ARNN, a new improved prediction model that achieves a 94% error reduction in forecasting. To determine the important environmental factors influencing air pollution, [3] make use of genetic algorithms. In case of [9] authors use logistic regression and autoregression (AR) to anticipate and monitor air quality. Autoregression forecasts future PM2.5 levels based on past trends, whereas logistic regression categorizes pollution status. Thus, by using localized, real-world atmospheric data the paper increases the accuracy of the model.

An 11-year dataset from Taiwan's Environmental Protection Administration (EPA) is used in [10] to allow for a long-term examination of trends in air quality. The large dataset improves forecast accuracy by accounting for seasonal fluctuations and other important factor, whereas [12] employs bibliometric analysis, examining more than 900 peer-reviewed publications from 1990 to 2022. This study charts thedevelopment of research trends, important contributors, and international cooperation in machine learning applications for air pollution studies rather than concentrating on direct air pollution predictions. Since [6] uses data on air pollution from 23 Indian cities over a six-year period, it is extremely pertinent to emerging countries where air pollution is a major public health issue.

Support Vector Machines (SVM), Random Forests, Stackin g Ensembles, Adaptive Boosting (AdaBoost), and Artificial Ne ural Networks (ANN) are among the machine learning method s that are assessed in [10]which comes to the conclusion that AdaBoost is best at reducing mean absolute error (MAE), whi le the Stacking Ensemble model is the most successful, obtaini ng the highest R2 and lowest RMSE. But in case of methodology [12] offers a meta-analysis of research trends in air pollution prediction rather than implementing machine learning models. The report underlines the increasing importance of particulate matter prediction and lists important approaches utilized in the field. Gaussian Naive Bayes, Support Vector Machine, XGBoost, and five other machine learning models are compared in [6]. According to the study, XGBoost outperforms Gaussian Naive Bayes, which is efficient but lacks predictive precision, in terms of air pollution level prediction.

Though it could be enhanced with real-time data integration and wider geographic coverage, [10] provides a useful guidance for choosing machine learning models based on performance measures. Although[12] is a useful tool for scholars and decision-makers, the lack of forecasting models makes it inapplicable in the actual world. In the case of [6], the authors successfully apply machine learning to actual data, it would profit from more in-depth deep learning research as well as the inclusion of outside variables like the weather and legislative changes.

(ii) Analysing Health consequences from Ai pollution.

In order to observe the long-term, real-world consequences of air pollution on mental health, this [4] uses a natural experiment. Researchers can investigate the effects of pollution over time in an unaltered, natural environment by conducting a natural experiment. Participants are tracked

for ten years. According to the study, there is a direct link between air pollution and clinical depression, with even slight increases in pollution being associated with a nearly 1% higher risk of getting depression. Long-term mental health results are highlighted here.

Whereas, Panel data regression is used in [5], and data from the China Family Panel Surveys (2010 and 2014) are used. The study [5] uses a sizable sample size (52,568 observations) to investigate the connection between mental health and air pollution. According to the [5], which measures mental health using the CES-D scale, there is a modest decline in CES-D scores for every 1 µg/m3 increase in PM2.5, which may indicate a detrimental effect on mental health. This study also shows that smokers and those with lower incomes are more susceptible to the negative effects of air pollution on mental health.

Because the study's [4] primary focus is clinical depression, it might not adequately account for the variety of mental health consequences associated with air pollution, such as anxiety, stress, and cognitive deterioration. In contrast to study [5], Study [4] doesn't address how pollutants and personal habits like smoking and exercise may combine to impact mental health. The study [5] examines smoking, but it skips over other health behaviors (such as diet and exercise) that may alter the relationship between pollution and mental health. Potential confounding factors, such as genetic predisposition or other environmental stresses that can influence the relationship between pollution and mental health outcomes are disregarded in this study.

Panel data regression is used in [5] on a large dataset that includes 52,568 observations from the China Family Panel Surveys (CFPS) conducted between 2010 and 2014. The study focuses on PM2.5 concentrations as a measure of air pollution and the CES-D scale to assess mental wellbeing. According to key findings, CES-D scale scores dropped by 0.012 for every 1 µg/m3 increase in PM2.5 concentration, indicating deteriorating mental health. The study also finds that smoking makes the detrimental impacts of air pollution on mental health worse, with low-income populations being more at risk.

Whereas, [11] employs a prospective longitudinal methodology, tracking 1,698 people in South East London over a five-year span (2008–2013). The impact of several air pollutants, such as NO2, NOx, O3, PM10, and PM2.5, on mental health outcomes is assessed in this study. The authors adjust for socioeconomic and environmental variables, such as exposure to traffic noise, and employ high-resolution air pollution data that is connected to the individuals' residential locations. The main conclusions of [11] demonstrate that while PM10 has the largest correlation with psychotic experiences (33% increase), elevated levels of PM2.5, NOx, and NO2 are linked to an 18–39% higher chance of mental health problems. The study emphasizes in particular that there were higher correlations between continuing pollution exposure and declining mental health among those who did not move during the study period.

[5] has certain limitations even if it successfully illustrates the long-term effects of PM2.5 exposure on mental health. Because it is observational in nature, it does not demonstrate causality, it does not include information on health behaviors other than smoking, and it leaves out potential confounding variables that might influence the relationship between pollution and mental health. While [11] suggests that their results have implications for public health and urban planning policy, indicating that enhancing the quality of the air in busy places may significantly improve mental health.

(iii) Analysing methods used for prediction of air pollution using deeplearning.

The main focus of [7] was Predicting air pollution levels (PM2.5) in Beijing but in [8] the authors concentrated on Identifying and classifying visual pollution in urban Dhaka, and in [13] authors contributed an innovative way of detecting air pollution by detecting and categorizing visual pollution on public highways. Different sorts of methodology was implemented in the three papers: [7] was used Hybrid CNN- LSTM deep learning model using meteorological and historical pollutant data, [8] used Deep learning-based object detection (YOLOv5, YOLOv7, Faster SegFormer) with Google Street View and [13] used Deep Active Learning (DAL) with YOLO- based VPP system for real-time detection.

While all three research employ deep learning to monitor the environment, Study [7] uses hybrid models to forecast air pollution, while research [8] and [13] use high-precision classification models to identify visual pollution. Study [13] incorporates deep active learning to increase accuracy and efficiency, whereas Study [8] offers a novel, inexpensive real- time solution. While Studies [8] and [13] support infrastructure management and urban aesthetics, In Study [7] author's forecasting methodology has a significant impact on public health. Future studies should look into combining thesestrategies and using hybrid AI models for real-time interventions and multi-dimensional pollution analysis.

III. CONCLUSION

Air pollution continues to pose a serious risk to public health, impacting both mental and physical health. The way we evaluate and react to pollution has been completely transformed by the use of machine learning into air quality monitoring and prediction. Researchers and policymakers can create more precise forecasting systems that allow for prompt responses and improved urban planning by utilizing sophisticated models and data-driven methodologies.

All of the papers that were evaluated highlight how seriously air pollution affects public health, especially when it comes to its association with mental health issues. Predicting air quality and monitoring the environment have been greatly improved by the application of machine learning models and new technologies, which present encouraging ways to reduce pollution in urban areas. Policymakers and researchers may create better early warning systems and intervention plans to safeguard public health and enhance urban air quality management by utilizing these cutting-edge techniques.

REFERENCES

[1] Dixian Zhu, Changjie Cai, Tianbao Yang and Xun Zhou, “A Machine Learning Approach for Air Quality Prediction: Model Regularization and Optimization,” Big data and cognitive computing, 2018.

[2] Mauro Castelli ,Fabiana Martins Clemente, AleˇsPopoviˇ, Sara Silva, and Leonardo Vanneschi, A Machine Learning Approach to Predict Air Quality in California, Hindawi Complexity Volume 2020, 2020.

[3] Mahmoud Reza Delavar, Amin Gholami, Gholam RezaShiran,Yousef Rashidi Gholam Reza Nakhaeizadeh, Kurt Fedra and Smaeil Hatefi Afshar, “A Novel Method for Improving Air Pollution Prediction Based on Machine Learning Approaches: A Case Study Applied to the Capital City of Tehran”, Internation journal of geo information, 2019

[4] Younoh Kim, James Manley, and Vlad Radoias, “Air Pollution and Long Term Mental Health”, Antony.D, MDPI, 2020.

[5] Zhiming Yang, Qianhao Song, Jing Li, Yunquan Zhang, Xiao-Chen Yuan, Weiqing Wang and Qi Yu, “Air pollution and mental health: the moderator effect of health behaviors”, Environmental Health Letters, 2021.

[6] K. Kumar, B. P. Pande, “Air pollution prediction with machine learning: a case study of Indian cities”, International Journal of Environmental Science and Technology, 2022

[7] Abdellatif Bekkar, Badr Hssina, Samira Douzi and Khadija Douzi“, Air pollution prediction in smart city, deep learning approach”, Journal of Big Data, 2021.

[8] Md Fahim ShahoriarTitu , Abdul Aziz Chowdhury , S. M. Rezwanul Haque and Riasat Khan, “Deep-Learning-Based Real-Time Visual Pollution Detection in Urban and Textile Environments”, MDPI, 2024.

[9] Aditya C R, Chandana R Deshmukh, Nayana D K, , Praveen Gandhi Vidyavastu “Detection and Prediction of Air Pollution using Machine Learning Models”, International Journal of Engineering Trends and Technology, 2018

[10] Yun-Chia Liang, Yona Maimury, Angela Hsiang-Ling Chen and Josue Rodolfo Cuevas Juarez, "Machine Learning-Based Prediction of Air Quality", MDPI, 2020.

[11] Ioannis Bakolis, Ryan Hammoud, Robert Stewart, Sean Beevers, David Dajnak, Shirlee MacCrimmon, Matthew Broadbent, Megan Pritchard, NarushigeShiode, Daniela Fecht, John Gulliver, Matthew Hotopf, Stephani L. Hatch, Ian S. Mudway, "Mental health consequences of urban air pollution: prospective population based longitudinal survey", Social Psychiatry and Psychiatric Epidemiology, 2020.

[12] Shikha Jain, Navneet Kaur, Sahil Verma, Kavita, A.S. M. Sanwar Hosen, and Satbir S Sehgal, "Use of Machine Learning in Air Pollution Research: A Bibliographic Perspective", MDPI, 2022

[13] Mohammad AlElaiwi, Mugahed A. Al-antari, Hafiz Farooq Ahmad, Areeba Azhar, Badar Almarri and Jamil Hussain, "VPP: Visual Pollution Prediction Framework Based on a Deep Active Learning Approach Using Public Road Images", MDPI, 2022

A STUDY ON DERMATOLOGICAL DIAGNOSIS OF CARDIOVASCULAR DISEASE THROUGH MULTIMODAL FUSION OF ARTIFICIAL INTELLIGENCE

*Albert Irudaya Raj J** [1], *K. Lakshmi Priya* [2]

ABSTRACT

The incorporation of multimodal fusion of Artificial Intelligence (AI) has the feasible to improve the dermatological diagnosis of cardiovascular diseases (CVDs). This survey reviews recent advancements in AI techniques that utilize diverse data types, including dermoscopic images, electronic health records (EHRs), to enhance diagnostic accuracy. Drawing from Scopus-indexed journals, we present a comprehensive literature review, discuss methodologies and approaches, and highlight recent trends in the field. This synthesis of knowledge aims to inform future research directions and promote interdisciplinary collaboration.

Keywords: Multimodal Fusion, Artificial Intelligence, Dermatology, Cardiovascular Disease, Diagnostic Accuracy, Machine Learning

I. INTRODUCTION

The potential usage of Artificial Intelligence in healthcare is huge and especially Dermatological diagnosis of various skin problems[4]. The AI dermatolodiagnosis of particular skin conditions status will reflect in quick prediction of cardiovascular diseases is one of the significant advancements for early detection. The Fusion of multimodal AI which includes integrating various data sources presents a novel approach to enhancing diagnostic processes. This paper aims to review current literature on the application of multimodal AI in dermatology, focusing on methodologies, approaches, and emerging concepts to improve cardiovascular disease diagnosis

Department of Information Technology[1]
Arul Anandar college (Autonomous), Karumathur,Madurai[1]
albert.irudaya@gmail.com[1]
Department of Computer Science[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
akshmipriyak.krishnan@kahedu.edu.in[2]

* Corresponding Author

II. LITERATURE REVIEW

A. Pitfall Models in Developing Mutimodals

From the following Paper[3] Journal of Medical Internet Research Solutions to presisting issues, in terms of excellences, such as collecting Precise data, enhancing practice, rexamine bulk data, improving instance size, preventing over fitting using data methods, using particular algorithms of Artificial Intelligence to address Sepcific problems.

B. Role of Dermatological Indicators in CVD

Research highlights several skin conditions, such as xanthomas and cyanosis, that serve as markers for underlying cardiovascular issues. Studies emphasize the need for AI systems to recognize these indicators effectively. The following paper clearly review that, people having Psoriasis have high Risk factor for Cardiovas family possible of early heart disease. A study seems to be published in the Journal of Investigative Dermatology (2022), people with psoriasis had more risk of CVD analysed to the general population (hazard ratio: 1.34, 95% CI: 1.14- 1.57) [6]

Here the Person whose age at 35, where our methods covers the elbows, interior shins, and lower abdomen (covering >10% of his body), which has cleared with an inter leukin (IL) various obstacle. The Person who had not smoke and no as the elbows, anterior shins, and lower abdomen (wrapping >10% of his body), which has cleared with an inter leukin (IL) of various obstacle.

The Male Person around 50-year old comes to your office to begin care. His previous psoriasis history starts at 35 years of age, previously known Cardiovascular. [4]

Data Acquisition:

Collect a diverse dataset comprising skin images, demographic information, and clinical records of individuals with and without CVDs.

A. Data Preprocessing:

Preprocess skin images to enhance image quality and remove noise.

B. Deep Learning Techniques

Recent studies have demonstrated high accuracy in diagnosing skin conditions related to cardiovascular health [4]. The concepts of Deep Learning, and convolutional neural networks (CNNs), has shown promise in analyzing dermatological images.

C. Integration of Clinical Data

The incorporation of clinical data from EHRs alongside picture data has been linked to improved diagnostic outcomes. Research indicates that integrating these data sources can enhance the contextual understanding of dermatological symptoms.[7]

D. Physiological Signal Analysis

Studies employing physiological signal analysis, such as heart rate variability, highlight the importance of real-time monitoring in assessing cardiovascular risk through dermatological evaluations. [9]

E. Interdisciplinary liaison

This will improve our understanding of the association between the two important systems

F. Multimodal Fusion

Combine the uprooted features from distinct plan using appropriate bending strategies, such as early fusion, late fusion, or hybrid fusion.

G. Model Development and Training

We need to focus on various models such as machine learning, support the following concepts vector machines (SVMs), random forests, or deep neural networks, on the fused feature set.

III. RECENT TRENDS

Diverse cardiac problem in present days as common and quick treatment solutions which result in dermatological expose which may furnish major symptoms to the curcial disease. This Journal paper, will let us know the important of dermatological symptoms which replicate in our cardiac conditions. Each and every one understand this collaborative concept will improve our diagonising pattern between the dermatological and cardiovascular systems in the essential infection cure.

Recent trends indicate:

Tele dermatology: Increasing use of remote consultations and AI-assisted diagnostics.

Wearable Technology: Integration of wearable devices to monitor physiological changes and their dermatological manifestations.

Personalized Medicine: AI models tailored to individual patient data, enhancing diagnostic accuracy and treatment plans.

IV .CARDIAC DISORDERS WITH DERMATOLOGICAL MANIFESTATIONS

Endocarditis:

Janeway Lesions: we can said through Painless macules on palms and soles.

Osler Nodes: here we usage the Painful nodules on fingers.

Atherosclerosis:

Xanthomas: Yellowish lesions due to lipid deposits, often associated with familial hyperlipidemia.

Arcus Senilis: A gray or white arc around the cornea, indicating lipid accumulation.

1. Heart Failure:

Cyanosis: The exitsting mucous membranes due to poor circulation or oxygenation. [7]

Clubbing: Enlargement all the fingertips and toes, potentially indicating chronic hypoxia.

2. Systemic Conditions

Malar Rash: A butterfly-shaped rash that may indicate underlying autoimmune disorders affecting the heart.

Dermatomyositis: Associated with underlying malignancies and can present with heliotrope rash and Gottron' s papules.

3. Hyperlipidemia:

Cutaneous Lipid Deposits: May appear as yellowish

plaques (xanthelasma) around the eyelids.

4.1 Importance of Interdisciplinary Collaboration

Holistic Patient Care: Understanding the connections between skin signs and cardiac conditions can enhance diagnostic accuracy and treatment efficacy.

Shared Knowledge: Dermatologists and cardiologists can benefit from each other' s insights, leading to better patient outcomes.

4.2 Classification of Dermatological Conditions

1. Traditionally CVR-Associated Conditions

Psoriasis: Inflammatory nature linked to atherogen. Associated risk factors: obesity, hypertension, and dyslipidemia. [1]

Hidradenitis Suppurativa: Chronic inflammatory skin condition with a strong correlation to metabolic syndrome. Shared pathways with cardiovascular inflammation.

2. Lesser-Known Associations:

Atopic Dermatitis is Emerging data suggest links to metabolic syndrome, though the connection is less established. Seborrheic Dermatitis May beassociated with systemic diseases that increase CV risk, although the direct link remains unclear. Chronic Urticaria is Potential links due to chronic inflammation.

4.3 Mechanisms Linking Skin and Cardiovascular

Healt, Inflammatory Pathways: Discuss common proactive moderator (e.g., TNF- alpha, IL-6) that contribute to both skin and cardiovascular diseases.

Metabolic Factors: Highlight how conditions like obesity and insulin resistance affect both skin health and cardiovascular risk. [8][10]

4.4 Implications for Clinical Practice

Risk Factor Screening:

Encourage dermatologists and primary care providers to screen for traditional cardiovascular risk factors in patients with inflammatory skin conditions[2].

Interdisciplinary Collaboration:

Stress the importance of communication between dermatologists and cardiologists to manage patients holistically. [3]

Patient Education:

Emphasize educating patients about the importance of managing skin conditions not just for skin health but for cardiovascular prevention[5].

Mechanisms Underlying Cardiotoxicity

Inflammatory Pathways:

Explain how systemic inflammation may exacerbate cardiovascular risk, particularly in chronic skin conditions[11].

Metabolic Effects:

Discuss how certain medications can influence weight, lipid profiles, and blood pressure, thereby affecting cardiovascular health. Patient-Specific Risk Factors Importance of assessing existing conditions (e.g., hypertension, diabetes) before initiating[12].

Patient-Specific Risk Factors

Importance of assessing existing conditions (e.g., hypertension, diabetes) before initiating treatment. Identify how older age and additional comorbidities can amplify risks. Consideration of individual patient genetics and their potential impact on drug metabolism and cardiovascular outcomes.

Optimizing Therapeutic Regimens

Recommendations for regular cardiovascular assessments in patients on systemic therapies. Encourage collaboration between dermatologists and cardiologists for comprehensive management. Discuss strategies for balancing dermatologic needs with cardiovascular safety, such as choosing lower-risk medications or adjunctive therapies.

V. DISCUSSION

Here the multiple types of data can be taken as input. In that time the integration of different Modalities is a challenging issue, because of different parameters.

We need to combine all the parameters of Cardiovascular problem identified through dermatology is for deep analysis of Multi Data Sets, Clinical Images, Patient history, laboratory results of Dermatology. Finally, we can have the identify the cardiovascular through dermatology.

$\sum$=Ds+Ci+ph+lres

Where DS=Data Sets

Ci=Clinical Images Ph=Patient History Lres=Laboratory Results

VI. CONCLUSION

The fusion of multimodal AI in enhancing dermatological diagnosis of cardiovascular diseases predicts the early stages of cardiovascular diseases. The literature indicates significant advancements in methodologies and approaches, although challenges remain. Future research should focus on overcoming these problems faced through interdisciplinary collaboration and standardization of practices.

The fusion of multimodal AI in enhancing dermatological diagnosis of cardiovascular diseases predicts the early stages of cardiovascular diseases. The literature indicates significant advancements in methodologies and approaches, although challenges remain.

REFERENCES

[1] Anderson, F., "Personalized medicine in Dermatology: Leveraging AI for enhanced patient care", Journal of Personalized Medicine, 13(5), 324-339, 2023.

[2] Yu-Qing Cai, Da-Xin Gong, Li-Ying Tang, Yue Cai, Hui-Jun Li, Tian-Ci Jing, Mengchun Gong, Wei Hu, Zhen-Wei Zhang, Xingang Zhang, Guang-Wei Zhang, " Pitfalls in Developing Machine Learning Models for Predicting Cardiovascular Diseases: Challenge and Solutions" Journal of Medical Internet Research J July 2024, Med Internet Res 2024;26:e47645, doi:10.2196/47645.

[3] Rawan AlSaad, Alaa Abd-alrazaq, Sabri Boughorbel, Arfan Ahmed, Max-Antoine Renault, Rafat Damseh, Javaid Sheikh "Multimodal Large Language Models in Health Care: Applications, Challenges, and Future Outlook" , Journal of Medical Internet Research, Vol 26, Sep 2024, doi:10.2196/59505

[4] Michael S Garshick, Nicole L Ward, James G Krueger, Jeffrey S Berger, " Cardiovascular Risk in Patients With Psoriasis" , American College of Cardiology Foundation, pages 1670-1680, Vol 77 Issue 13, April 2021

[5] Kipp W. Johnson, Jessica Torres Soto, Benjamin S. Glicksberg, Khader Shameer, Riccardo Miotto, Mohsin Ali, MPHIL, Euan Ashley, Joel T. Dudley, "Artificial Intelligence in Cardiology", Journal of the American College Of Cardiology, VOL. 71, June, 2018.

[6] Andrew Hughes, Mobashir Hasan Shandhi Hiral Master, Jessilyn DunnEvan Brittain, " Wearable Devices in Cardiovascular Medicine" Circulation Research, Volume 132, Issue 5, 3 March 2023. https://doi.org/10.1161/CIRCRESAHA.122.322389

[7] Biyanka Jaltotage , Juan Lu, Girish Dwivedi, "Use of Artificial Intelligence Including Multimodal Systems to Improve the Management of Cardiovascular Disease", Canadian Journal of Cardiology, Volume 40, Issue 10, October 2024, https://doi.org/10.1016/j.cjca.2024.07.014

[8] Naiela E Almansouri, Selvambigay Rajavelu, Mishael Awe, Kudapa Jahnavi , Rohan Shastry, AliHasan, HadiHasan, Mohit Lakkimsetti, Reem Khalid AlAbbasi, Brian Criollo Gutiérrez, Ali Haider,, "Early Diagnosis of Cardiovascular Diseases in the Era of Artificial Intelligence: An In-Depth Review", Cureus Part of Springer Nature, March 2024 doi: 10.7759/cureus.55869.

[9] Ciccarelli, Michelea; Giallauria, Francescob; Carrizzo, Albinoa,c; Visco, Valeriaa; Silverio, Angeloa; Cesaro, Arturod; Calabrò, Paolod; De Luca, Nicolae; Mancusi, Costantinoe; Masarone, Danielef; Pacileo, Giuseppef; Tourkmani, Nidalg,h; Vigorito, Carlob; Vecchione, Carminea,c. "Artificial intelligence in cardiovascular prevention: new ways will open new doors" , Journal of Cardiovascular Medicine, May 2023, DOI: 10.2459/JCM.0000000000001431.

[10] ALuisa Soares1, Tatiana Leal2, Ana Lucia Faria3, Ana Aguiar4 and Catia Carvalho5. “Cardiovascular Disease: A Review”, Biomedical Journal of Scientifica & Technical Research, ISSN: 2574 - 1241, July 2023s, DOI: 10.26717/BJSTR.2023.51.008101.

[11] Alan D. Kaye, Rahib K. Islam, Victoria T. Tong, Elizabeth McKee, Julian J. Gonzales, Mohammed S, Rais, Abigail E. Watson, Christopher J. Haas , Ryan Chan, Zachary Palowsky, Kazi N. Islam, Sahar Shekoohi, Giustino Varrassi, “Cutaneous Dermatologic Manifestations of Cardiovascular Diseases: A Narrative Review”, Cureus Part of Springer Nature, October 24, 2024, doi:10.7759/cureus.72336. Andreas Triantafyllidis, “Deep Learning in mHealth for Cardiovascular Disease, Diabetes, and Cancer: Systematic Review” JMIR mHealth and uHealth, Apr 2022, doi: 10.2196/32344.

IoT BASED SECURE TRANSACTION IN REMOTE PATIENT MONITORING USING CRYPTOGRAPHY TECHNIQUES

*C.Preethika** [1], *E.J.Thomson Fredrik* [2]

ABSTRACT

Remote patient monitoring involves using technology to collect health data from individuals in one location and electronically communicating that information to healthcare sources in aaltered location. This allows healthcare professionals to monitor patients' conditions remotely. Health data collected by IoT devices are transmitted over the internet. While data transaction, security challenges are faced in remote patient monitoring .Safeguarding sensitive patient information is crucial to prevent from unauthorized access. In this article purpose cryptographic algorithm is used to prevent data during transaction,AES (Advanced Encryption Standard) and Blowfish algorithm is used in a hybrid encryption approach for securing data in remote patient monitoring. In this paper, IoT devices like SPO2 (blood oxygen saturation), temperature, and heart pulse sensors involves the continuous collection and transmission of vital signs from patients to healthcare providers. The integration of wearable devices and a secure remote monitoring system enhances the ability to detect and address medical issues promptly.Using a hybrid encryption approach with both AES and Blowfish can enhance security, mitigate various Cyber Attack and can do secure transaction in IoT. This combination helps protect against attacks such as brute-force attacks, cryptanalysis, and vulnerabilities specific to each algorithm. Additionally, it adds an extra layer of defense by diversifying the encryption methods, making it more challenging for attackers to exploit potential weaknesses in a single algorithm. The implementation result of this hybrid algorithm ensures confidentiality, integrity, authentication and trust in remote patient monitoring systems. In essence, the future of secure transactions in remote patient monitoring lies in a dynamic, adaptive approach that integrates cutting-edge technologies to fortify the overall cybersecurity posture and safeguard patient data with the highest level of resilience.

Keywords: Advanced Encryption Standard, Blow fish, Cryptography, Healthcare, Hybrid encryption, Internet of Things(IoT)

I. INTRODUCTION

IoT refers to the network of interconnected physical devices that communicate and exchange data over the internet to enhance various aspects of patient care, monitoring, and management. devices, equipped with sensors and connectivity, can collect, share, and act upon information to enable smart applications and services in various domains. IoT devices in remote patient monitoring offer real-time health data, enabling timely interventions, reducing hospitalizations, enhancing patient independence, and providing healthcare professionals with comprehensive insights for personalized care. This interconnected network of devices facilitates the collection and exchange of health-related data, promoting efficiency and improving patient outcomes. IoT in healthcare aims to improve patient outcomes, enhance preventive care, streamline processes, and provide more personalized and efficient healthcare services.

Temperature Monitoring monitors the patient's body temperature is crucial for identifying potential infections, inflammatory conditions, or abnormalities and helps in assessing the effectiveness of treatments and interventions. Digital thermometers or wearable temperature sensors. Continuous temperature monitoring aids in early detection of fever or hypothermia, enabling timely medical interventions. SPO2 (Oxygen Saturation) Monitoring measures the percentage of oxygen saturation in the patient's blood, indicating how well oxygen is being transported to the body's

Department of Computer Technology[1]
Karpagam Academy of Higher Education, Coimbatore, India[1]
preethi150702@gmail.com[1]
Department of Computer Technology[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
thomson500@gmail.com[2]

* Corresponding Author

tissues. It's crucial for assessing respiratory function and detecting conditions like hypoxemia. Continuous SPO2 monitoring is vital for early detection of respiratory distress, especially in patients with respiratory conditions. Heart Pulse Monitoring measures the heart rate, providing insights into cardiovascular health and overall cardiac function. It's essential for detecting irregularities, arrhythmias, or abnormal heart rates .Continuous heart pulse monitoring assists in early identification of cardiac issues, enabling prompt medical attention. While sharing a data from IoT devices to Website, security issue is the most common problem in using remote patient monitoring.

Some of the specific challenges are confidentiality, data integrity, key management, resistance to attacks, adaptability, performance, quantum resistance, and secure communication issues in the context of remote patient monitoring (RPM).

Addressing these issues requires a comprehensive security strategy and privacy of patient data in remote monitoring scenarios. AES and Blowfish are commonly used symmetric key encryption algorithms that can be employed together as part of a hybrid encryption approach to provide a more secure and efficient encryption process. AES is known for its speed and strong security, making it suitable for encrypting larger volumes of data efficiently. The remaining sections are literature review, proposed work, methodology, result and discussion, conclusion and future work.

II. LITERATURE REVIEW

IOT devices like temperature, heart pulse, blood pressure and oxygen meter are used to measure the real time data of the patients in healthcare. An alert system is used for the timely detection and notification of abnormal health parameters, enabling swift medical intervention to prevent or address potential health complications. Using an alert system cause the possibility of false alarms, Which an lead to unnecessary anxiety for the patient and healthcare providers, as well as potential overuse of medical resources. [1]

Wireless sensor network is mainly used for data assortment in remote patient monitoring. Wireless sensor networks facilitate seamless data collection in remote patient monitoring by deploying sensors to measure vital signs and transmit real-time health data wirelessly. Wireless communication introduces security considerations. [2]

Sensors are used to collect real time patient data, and helps healthcare providers assess and manage patients from distance. This enables healthcare professionals to remotely monitor patients, ensuring timely interventions and personalized care. This interference may lead to signal degradation, data packet loss, or even temporary loss of connectivity between the wireless sensors and the monitoring system. [3]

Automation through RFID tags reduces the risk of errors associated with manual data entry. By scanning RFID tags, healthcare providers can access accurate and up-to-date patient information, minimizing the chances of administering the wrong medication or treatment. RFID tags transmit and store patient information wirelessly. If proper security measures are not in place, there is a risk of third party access to this personal data. Without robust encryption and authentication protocols, RFID data may be susceptible to hacking or interception. [4]

Certificate less public key cryptography eliminates the need for digital certificates, streamlining key management processes. In traditional public key infrastructures, digital certificates are used to verify the authenticity of public keys. Certificate less public key cryptography is not as standardized as traditional public key infrastructure (PKI) systems that rely on digital certificates. The lack of standardized protocols can lead to interoperability challenges when integrating different systems or devices. [5]

Using genomic data and chaos theory for encryption in remote patient monitoring can provide a high level of security. Genomic data, being unique to individuals, adds a personalized layer of encryption. Chaos theory introduces further safeguarding sensitive health information. Disadvantage of using genomic and chaos as an encryption method in remote patient monitoring is the potential for increased computational complexity. Analyzing genomic

data and implementing chaos-based algorithms may require significant computational resources, leading to slower processing times and potential challenges in real-time monitoring scenarios. [6]

AES is a widely adopted and standardized encryption algorithm, known for its robustness and efficiency. Regular key management practices are crucial to mitigate this risk and maintain the effectiveness of AES encryption.[7]

Block chain offers advantages like data integrity and decentralized control. Using block chain in monitoring comes with challenges like scalability issues, high energy consumption and complexity. [8]

Blow fish as individual algorithm provides strong encryption, enhancing the security of sensitive patient data during transmission. Blow fish is an older encryption algorithm, and while it's still secure the fixed key size may limits its adaptability. [9]

Cryptographic algorithms are essential for securing financial transactions, authentication processes, and other critical operations in cloud based applications. Managing cryptographic keys in the cloud can be more complex than in traditional databases. Key distribution, rotation, and secure storage become challenging, and any compromise in key management can lead to security vulnerabilities. [10]

A database like PREDICT RM may incorporate predictive analytics algorithms. These algorithms can analyse patient data over time, identifying patterns and trends that may indicate potential health issues or deterioration in a patient's condition. Patients and healthcare providers need assurance that their data is protected against cyber threats and unauthorized use.[11]

During Pandemic time like COVID-19, Remote patient monitoring will be more helpful like finding first stage of COVID like, monitoring Heart pulse, oxygen level and temperatures. Patients may worry about the security of their health information, leading to hesitancy in adopting remote monitoring technologies. [12]

Disruption Tolerant Networking is used to ensure data delivery even in scenarios with intermittent or unreliable network connectivity. While DTN is designed to handle intermittent connectivity, the inherent delay-tolerant nature of the network may lead to slower data delivery. In time-sensitive healthcare situations, such delays could impact the promptness of medical interventions or decision-making based on real-time patient data. [13]

While Arduino and Proteus are popular tools for prototyping and small-scale projects, they may face limitations in terms of scalability when it comes to large-scale and robust remote patient monitoring systems. Building and maintaining a scalable, enterprise-grade solution for remote patient monitoring often requires professional support, specialized hardware, and dedicated software platforms. [14]

It can be prevented using Block chain encryption .While Block chain provides decentralized security features, it may not be the most efficient choice for remote patient monitoring due to its inherent complexity, performance overhead, and scalability challenges compared to dedicated encryption. [15]

In IoT based healthcare the design and implementation are discussed in this paper. This limitation can affect the device's ability to handle advanced data analytics, real-time processing, or support multiple sensors simultaneously, potentially impacting the overall performance and responsiveness of the monitoring system. [16]

DS18B20 temperature sensor with Arduino is used for health monitoring. It can measure body temperature, ambient temperature, or other relevant data. Connect the DS18B20 to the Arduino and can monitor temperature readings. But, Factors such as self-heating or response time variations in the DS18B20 may affect its performance in dynamic environments. This could be a consideration in scenarios where rapid changes in temperature need to be monitored accurately. [17]

The Thing Speak library for Arduino is commonly used in remote patient monitoring. Thing Speak library to send data from sensors (e.g., temperature, heart rate) connected to an Arduino to the Thing Speak platform. This enables remote monitoring, data logging, and real-time visualization through charts and graphs. However, when using a third-party cloud service like Thing Speak, there may be concerns related to data privacy and security. [18]

Tele health is used for connecting with your health care provider online safe and secure. Access to high-quality healthcare facilities and improved emergency services are among the better healthcare choices it provides. [19] Wireless Body Area Network implementation in remote patient monitoring involves utilizing wearable sensors to collect and transmit health-related data to a centralized system. These networks enable real-time monitoring and enhance healthcare delivery. The presence of other wireless networks, electronic devices, or physical obstacles may disrupt or weaken the communication signals between the body-worn sensors and the monitoring system. This interference can result in data packet loss, delays, or even complete communication failures. [20]

III. PROPOSED WORK

Using AES and Blowfish as a hybrid algorithm in remote patient monitoring offers several benefits compared to using individual algorithms. The combination provides a layered security approach, leveraging the strengths of both AES and Blowfish to enhance overall data protection. As data is collected from IoT sensors, the initial step involves encrypting this sensitive information using the Advanced Encryption Standard (AES). AES, known for its robust security and computational efficiency, ensures that the collected data remains confidential during transmission.. To address this, the hybrid approach incorporates Blowfish, a symmetric key algorithm with a distinct encryption process. The AES key is encrypted using Blowfish, adding an extra layer of security to the key exchange process. This hybrid encryption strategy combines the strengths of both algorithms—AES for efficient and secure data encryption and Blowfish for a protected key exchange mechanism. By leveraging AES and Blowfish in tandem, the hybrid algorithm helps safeguard sensitive patient data during its journey from IoT sensors to websites. This approach mitigates potential vulnerabilities associated with individual algorithms, providing a robust and well-rounded security framework for remote patient monitoring transactions in the evolving landscape of healthcare IoT.

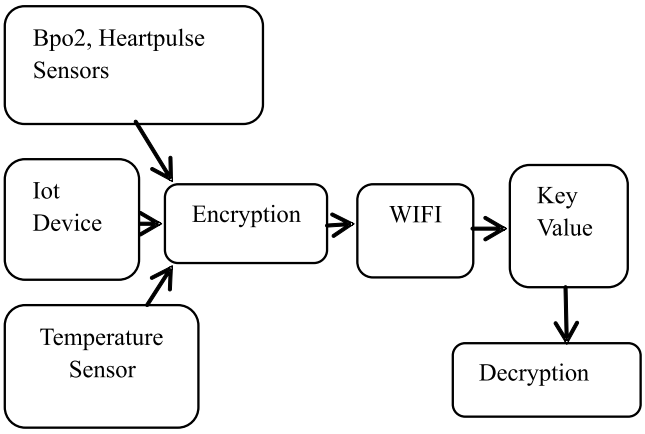

Figure 1. Block diagram of Secure Remote Patient Monitoring

IV. METHODOLOGY

Real time data was composed from IoT devices by using its sensors. The three IoT devices used for monitoring the patient's health conditions. It helps to monitors oxygen levels, crucial for respiratory health, and detects potential issues like hypoxemia. Temperature sensors track a patient's body temperature. Data is sent in real-time through IoT connectivity for continuous monitoring. It helps identify fever, a common symptom in various illnesses, providing early detection and intervention.DS18B20 is used as temperature sensor to get data from patient and helps in monitoring temperature level. Pulse sensors capture the heart rate of the patient. Transmitting heart rate data through IoT enables real-time monitoring by healthcare professionals. Monitor cardiovascular health, aids in identifying irregularities or abnormalities in heart rate.MAX30100 is also acting as heart rate sensor and helps to monitor the patient's heart rate. This sensor is used to get real time data for monitoring. MAX30100 and DS18B20 sensors are used for collecting the data of blood oxygen level, temperature, and heart pulse. The integration of SPO2, temperature, and heart pulse sensors as IoT devices in remote patient monitoring enhances healthcare by providing real-time data for better diagnosis, early intervention, and improved patient outcomes.

Arduino is an open-source electronics platform that combines programmable hardware with an easy-to-use

software environment. It consists of a microcontroller-based board and an Integrated Development Environment (IDE) for writing and uploading code. Designed to simplify microcontroller programming, Arduino provides an accessible and flexible framework for developers and hobbyists. Its adaptability makes it valuable in various fields, including healthcare, where it enables the development of innovative medical and assistive devices.

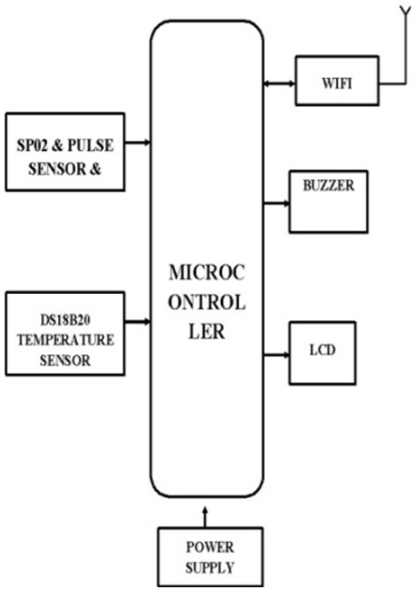

Figure 2. Methodology of overall circuit board

Buzzer is also connected to an Ardiuno board. A buzzer is a signaling device that consists of switches or sensors linked to a control unit. When a button is pressed or a set time elapses, the control unit activates a light on the corresponding button or panel. It then produces an alert through a continuous or intermittent buzzing or beeping sound.

For power supply, the proper operation of an electronic device or product, a reliable power supply unit (PSU) is essential. Built into the device, this power supply unit converts AC mains voltage to an appropriate level of DC voltage. The Switching Mode Power Supply (SMPS) is the most commonly used type of power supply circuit, efficiently transforming AC mains power to 12V DC with its designated current rating

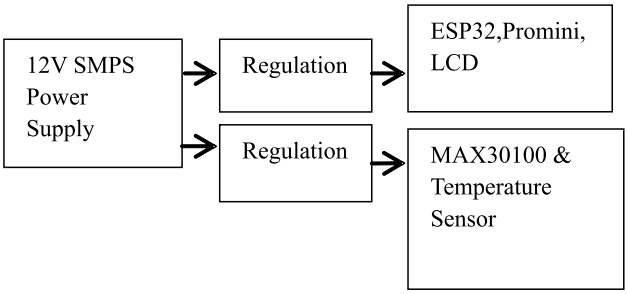

Figure 3. Power Supply between Sensor Board and Arduino Board

The ESP32, with its built-in Wi-Fi capabilities, can be utilized in various healthcare applications to enable connectivity, remote monitoring, and data transmission. This device enables real-time health data transmission to a website via Wi-Fi, facilitating remote patient monitoring and timely interventions. Compared to the ESP-12e, the ESP32 offers significant improvements, including a more powerful CPU, faster Wi-Fi connectivity, and additional GPIO pins, particularly for analog inputs. It also supports Bluetooth 4.2 and Bluetooth Low Energy. Moreover, the board features touch-sensitive pins and integrates built-in Hall Effect and temperature sensors.

The ESP-WROOM-32 is widely utilized in IoT applications because of its integrated Wi-Fi and Bluetooth features. It enables devices to establish internet connectivity and communicate wirelessly with other systems.

A. System Design

The ESP32, MAX30100, TEMPERATURE SENSORS require 3.3V while LCD, PRO-MINI use 5V DC for their operation and relay modules need 12V DC for their procedure. The ESP32 can operate using either a USB connection or a 12V adapter with a 5V DC regulated power supply. As the voltage supply and ground pins of other modules share a common VCC and ground, the components receive power from the regulator's 5V output. The system's LCD is connected to the I2C 21st and 22nd pins, enabling serial communication. A buzzer is linked to the digital 4th pin of the ESP32. The LCD display presents sensor-scanned values.

The temperature sensor is linked to 15th digital pin of esp32 as one wire communication input to monitor patient body temperature, system alerts if temperature value exceeds. MAX30100 SPO2 and HEART PULSE sensor is connected to Arduino pro-mini controller in order to continuously scan and send the spo2 and heart pulse value to ESP32 via UART Communication. ESP32 Reads SPO2 and Heart Pulse value and displays in LCD. Also alerts when Heart Pulse and SPO2 are in abnormal.All parameters can be monitored remotely using IoT (Internet of things) via online server by updating the entry of patient parameters every minute and also updates warnings online in any abnormal cases.

B. System Implementation

In RPM, the asymmetric algorithm may be used to exchange a symmetric key, enabling subsequent data encryption using a symmetric algorithm like AES or Blowfish. Before initiating data transmission, a symmetric key is generated for use in encrypting the sensitive patient information. Subsequently, the AES algorithm is employed to encrypt the patient health data, ensuring its confidentiality during transit. To address the secure exchange of the symmetric key, the AES key is further encoded using the Blowfish algorithm. This two-layered encryption process fortifies the key exchange mechanism, mitigating risks associated with potential interception.Once the encrypted data, along with the Blowfish-encrypted AES key, reaches its destination on the website, the decryption process is initiated. The Blowfish key, which was securely shared between the IoT devices and the server, is utilized to decrypt the AES key. Subsequently, the decrypted AES key is employed to decrypt the patient health data. This meticulous decryption process ensures that only authorized entities possessing the appropriate keys can access and interpret the sensitive health information. Ultimately, the hybrid algorithm's application of AES and Blowfish shows a pivotal part in preserving the reliability and privacy of patient data throughout the remote patient monitoring process.

V. RESULT AND DISCUSSION

Table 1: Decryption Data using AES and Blowfish algorithm

S.No	Date	Decrypted Temperature	Decrypted Heart Pulse	Decrypted spo2
1	08-03-2024 08:10:48	36	97	96
2	08-03-2024 08:09:33	36	100	96

In secure transaction of remote patient monitoring, we implemented a hybrid encryption approach utilizing the AES (Advanced Encryption Standard) and Blowfish algorithms. channel for transmitting sensitive patient health data. The encryption process effectively safeguarded the confidentiality and integrity of the information exchanged between remote patient monitoring devices and the central monitoring system.

By leveraging both AES and Blowfish, the system not only meets industry standards but also addresses the dynamic nature of IoT devices and the critical nature of health data. The encryption provided by this hybrid algorithm ensures confidentiality, integrity, and authenticity, essential pillars for maintaining trust in remote patient monitoring systems.

VI. CONCLUSION

From the result the implementing of hybrid algorithm with AES and Blowfish in remote patient monitoring offers a comprehensive solution for securing data during transactions from IoT devices to healthcare professionals. AES brings efficiency and widespread acceptance, ensuring swift encryption of vital signs such as temperature, BPO2, and heart pulse. Complementarily, Blowfish adds an extra layer of security with its unique algorithm, contributing to a robust defense against potential threats. In conclusion, the AES and Blowfish hybrid algorithm stands as a robust solution, effectively securing patient data transactions in the realm of remote healthcare monitoring. It's essential to keep these algorithms up-to-date and follow best practices in key management, protocol design, and implementation to ensure the highest level of security in remote patient monitoring systems. In essence, the future of secure transactions in remote patient monitoring lies in a dynamic, adaptive

approach that integrates cutting-edge technologies to fortify the overall cyber security posture and safeguard patient data with the highest level of resilience.

REFERENCES

[1] Warsi, G. G., Hans, K., &Khatri, S. K. (2019, February). IOT based remote patient health monitoring system. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 295-299).IEEE.

[2] Malasinghe, L. P., Ramzan, N., &Dahal, K. (2019). Remote patient monitoring: a comprehensive study. Journal of Ambient Intelligence and Humanized Computing, 10, 57-76.

[3] Hilty, D. M., Armstrong, C. M., Edwards-Stewart, A., Gentry, M. T., Luxton, D. D., &Krupinski, E. A. (2021). Sensor, wearable, and remote patient monitoring competencies for clinical care and training: scoping review. Journal of Technology in Behavioral Science, 6, 252-277.

[4] Ahmed, M. I., &Kannan, G. (2022). Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring. Journal of King Saud University-Computer and Information Sciences, 34(9), 6895-6908.

[5] Hamoud, O. N., Kenaza, T., Challal, Y., Ben-Abdelatif, L., &Ouaked, M. (2022). Implementing a secure remote patient monitoring system. Information Security Journal: A Global Perspective.

[6] Aledhari, M., Marhoon, A., Hamad, A., &Saeed, F. (2017, July).A new cryptography algorithm to protect cloud-based healthcare services. In 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) (pp. 37-43). IEEE.

[7] Sandhiya, D. S., Karthikeyan, M. V., &Priya, M. S. (2022). Secured Health Monitoring System Using AES. East Asian Journal of Multidisciplinary Research, 1(6), 1175-1182.

[8] Pighini, C., Vezzoni, A., Mainini, S., Migliavacca, A. G., Montanari, A., Guarneri, M. R., ...&Cesareo, A. (2021). SynCare: An innovative remote patient monitoring system secured by cryptography and blockchain. In IFIP International Summer School on Privacy and Identity Management (pp. 73-89). Cham: Springer International Publishing.

[9] Hussaini, S. (2020). Cyber security in cloud using blowfish encryption. Int. J. Inf. Technol.(IJIT), 6(5).

[10] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 354-361, doi: 10.1109/ICOEI48184.2020.9143018.

[11] Rajarathna, S. N. A Study on Different Types of Cryptographic Algorithms in Securing Cloud Based HealthCare Services.

[12] Hummel, J. P., Leipold, R. J., Amorosi, S. L., Bao, H., Deger, K. A., Jones, P. W., ... &Akar, J. G. (2019). Outcomes and costs of remote patient monitoring among patients with implanted cardiac defibrillators: an economic model based on the PREDICT RM database. Journal of Cardiovascular Electrophysiology, 30(7), 1066-1077.

[13] Sabukunze, I. D., Setyohadi, D. B., &Sulistyoningsih, M. (2021, April). Designing an Iot based smart monitoring and emergency alert system for Covid19 patients. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-5). IEEE.

[14] Yaacoub, E., Abualsaud, K., Khattab, T., &Chehab, A. (2020). Secure transmission of IoTmHealth patient monitoring data from remote areas using DTN. IEEE Network, 34(5), 226-231.

[15] Mihat, A., Saad, N. M., Shair, E. F., Aslam, A. B. N., & Rahim, R. A. (2022). SMART HEALTH MONITORING SYSTEM UTILIZING INTERNET OF THINGS (IoT) AND ARDUINO. Asian Journal Of Medical Technology, 2(1), 35-48.

[16] Pham, H. L., Tran, T. H., & Nakashima, Y. (2018, December).A secure remote healthcare system for hospital using blockchain smart contract. In 2018 IEEE

[17] Ashraf, S., Khattak, S. P., &Iqbal, M. T. (2023).Design and Implementation of an Open-Source and Internet-of-Things-Based Health Monitoring System. Journal of Low Power Electronics and Applications, 13(4), 57.globecom workshops (GC Wkshps) (pp. 1-6).IEEE.

[18] Saha, R., Biswas, S., Sarmah, S., Karmakar, S., & Das, P. (2021). A working prototype using DS18B20 temperature sensor and arduino for health monitoring. SN Computer Science, 2, 1-21

[19] P. GURUNATHAN and R. S. DEVI, "RSA Cryptography and GZIP Steganography Techniques for Information Hiding and Security using Java," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 654-659, doi: 10.1109/ICOEI56765.2023.10125906.

[20] Hartalkar, A., Kulkarni, V., Nadar, A., Johnraj, J., &Kulkarni, R. D. (2020, September).Design and development of real time patient health monitoring system using Internet of Things. In 2020 IEEE 1st International Conference for Convergence in Engineering (ICCE) (pp. 300-305). IEEE.

[21] Schultz, M. A. (2023). Telehealth and Remote Patient Monitoring Innovations in Nursing Practice: State of the Science| OJIN: The Online Journal of Issues in Nursing. Online Journal of Issues in Nursing, 28(2).

[22] Majeed, J. H., &Aish, Q. (2021). A remote patient monitoring based on WBAN implementation with internet of thing and cloud server. Bulletin of Electrical Engineering and Informatics, 10(3), 1640-1647.

MACHINE LEARNING FOR INTRUSION DETECTION: TRENDS, CHALLENGES AND FUTURE DIRECTIONS

Resmi Krishnan V [1], *S. Mythili* [2]

ABSTRACT

Networks and information systems must be protected from cyberattacks by intrusion detection systems. Traditional rule- based intrusion detection systems are becoming less and less effective against complex and dynamic threats. Consequently, machine learning (ML) approaches are being used to create more intelligent, flexible and instantaneous threat detection systems. The Machine learning approaches utilised in IDS are supervised, unsupervised, ensemble, deep learning and federated learning models which is thoroughly reviewed in this work. Their benefits, drawbacks and practical uses are highlighted. This study also covers performance evaluation measures, datasets and new developments including edge computing solutions, privacy- preserving intrusion detection systems and Explainable AI (XAI). The study offers possible remedies while shedding light on problems related to feature selection, class imbalance, scalability and false positives. This research aims to provide researchers and practitioners with a better understanding of recent advancements in IDS models.

Keywords: Intrusion detection system, Ensemble learning, Machine learning, Deep learning, Federated learning, Explainable AI.

I. INTRODUCTION

Since cyber attacks are becoming more frequent, vast and complicated protecting computer networks and information systems is a challenging issue in this digital era. Intrusion detection systems (IDS) are essential component of modern cyber security framework because they can only detect and prevent unlawful activities, policy violations, and potential network attacks. Traditional intrusion detection systems (IDS), which mostly rely on signature-based anomaly detection find it challenging and nearly failed to keep up with evolving threats like advanced persistent attacks (APT) and zero-day exploits. Due to this changing cyber threat landscape, there has been a surge in the use of machine learning (ML) algorithms that provide intelligent and adaptable capabilities to enhance the effectiveness of IDS.

Machine learning based intrusion detection systems utilize capacity to automatically recognize patterns in data and spot variations that can point to a malicious activity. These algorithms fall into three categories mainly ensemble, supervised, and unsupervised. Labelled datasets are used to train models in supervised approaches however lack their ability to identify invisible threats. On the other hand, unsupervised methods are appropriate for unidentified threats since they identify irregularities without requiring prior knowledge of attack patterns. Ensemble techniques overcome the limitations of individual models by combining several algorithms to increase detection accuracy. Despite these benefits Machine Learning - based intrusion detection systems encounter difficulties with feature selection, high false positive rates, scalability and real- time performance.

General Educational Department[1]
GGVHSS School, Nemmara, Palakad[1]
resmikishor2010@gmail.com[1]
Department of Computer Science[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
smythili78@gmail.com[2]

* Corresponding Author

Table 1: Machine Learning Algorithms In Ids

YEAR	NUMBER OF STUDIES/PAPERS USING ML TECHNIQUES	KEY MACHINE LEARNING METHODS HIGHLIGHTED
2019	20+	Traditional ML algorithms (e.g., SVM, Decision Trees, k-NN), initial hybrid models
2020	30+	Deep learning models like DBNs, CNNs, and autoencoders; focus on anomaly detection.
2021	40+	Federated learning, IoT-specific IDS, emphasis on feature engineering.
2022	50+	GANs, ensemble methods, real-time detection, cloud-based ML approaches.
2023	60+	Explainable AI (XAI), hybrid deep learning models, privacy-preserving IDS.
2024	70+	Advanced multi-layer neural networks, 5G and edge-computing IDS solutions.

With an emphasis on significant developments, constraints and unresolved research issues, this work attempts to present a thorough analysis of machine learning methods used in Intrusion Detection System. This study focusses on assessment metrics, different machine learning models such as federated learning, hybrid models, and deep learning and assess how well different approaches perform on benchmark datasets. This study aims to provide academicians and practitioners with useful insights by synthesizing data from previous studies, directing futureadvancements towards more reliable, flexible, and effective Intrusion Detection System solutions.

II. RELATED STUDIES

Due to increasing complexity of cyber-attacks, there has been a tremendous increase in the use of machine learning (ML) techniques in Intrusion Detection Systems (IDS) in recent years. Numerous studies have investigated various machine learning techniques such as supervised, unsupervised and ensemble methods to enhance IDS performance. Due to their superior ability to handle complex network data and invisible malicious attacks Deep learning (DL) models like auto encoders and convolutional neural networks (CNN) are becoming more popular. Initially, researchers concentrated on traditional Machine Language classifiers like decision trees, support vector machines, and k-nearest neighbors.

The use of machine learning in Intrusion Detection System (IDS) to solve security and privacy related issues on the Internet of Things is covered in the research [1]. Concept drift, high dimensional data and computational complexity are the major drawbacks with traditional intrusion detection models. The authors suggested that machine learning approaches is the only solution for such problems. The popular datasets examined by them for IDS development are Kyoto, NSL-KDD, and KDD99 highlighting the necessity of striking a balance between detection accuracy and computing efficiency in order to adjust to changing IoT contexts.

[2] compared different machine learning classifiers for intrusion detection systems (IDS). Moreover, this paper provides valuable information on how well the classifiers perform real time in terms of recall, accuracy, precision and training time. [3] describe a method for using Deep Belief Networks (DBNs) for anomaly detection in the Internet of Things (IoT).

An intrusion detection system (IDS) that uses auto encoders for accurate anomaly detection is presented in the research [4]. The study [5] suggested a hybrid intrusion detection system model for IoT environments which combines machine learning with anomaly-based and signature-based detection.[6] studied a modified clustering approach for improving intrusion detection framework. [7] studied the effectiveness of many deep learning architectures, including recurrent neural networks (RNNs) and convolutional neural networks (CNNs), at detecting intricate intrusion patterns in network traffic data.

The study by [8] focused on federated learning approaches for intrusion detection systems (IDS) in

distributed network environments. The study by [9] examines ensemble learning techniques for network intrusion detection and proved that ensemble methods can effectively reduce false positives and improve detection rates. The study by [10] aimed at developing intrusion detection systems based on adaptive learning strategies such as ensemble learning for improving network security.

[11] studied about real time intrusion detection system using deep learning techniques. Their study highlighted that real-time intrusion detection systems can be used for quickly identifying intrusions and deep neural networks can process massive data streams quickly with accuracy.

The study conducted by [12] provided organizations looking for real time security solutions for larger networks in cloud computing environment. The goal of [13] study is to assess classifiers like Decision Trees, Support Vector Machines and Neural Networks on various datasets to identify network hazards.

[14] study presents a unique intrusion detection system that uses auto encoder networks to detect unusual activity within network data. A comprehensive survey of supervised learning methods in intrusion detection system is given by [15] describe that classifier like Support Vector Machine, Random Forests and Neural Networks are employed to identify unknown attack patterns. [16] discussed the development of intrusion detection system designed specifically for edge computing environments.

Standardized datasets are essential for enhancing the effectiveness of intrusion detection systems according to study by [17]. For smart grids [18] presented a hybrid intrusion detection technique that increases detection precision. The hybrid model uses classification with Long Short-Term Memory (LSTM) networks and feature extraction with XGBoost and Convolutional Neural Networks (CNNs). Generative Adversarial Networks (GANs), which create possible attack scenarios and model data distributions was used by [19] to present an anomaly-based intrusion detection system.

The research by [20] examines feature reduction techniques for real-time intrusion detection systems, including methods like Principal Component Analysis (PCA) and auto encoders to enhance performance by lowering computational demands while maintaining accuracy. [21] study underscore the versatility of deep learning and ensemble methods across different network environments, especially in reducing false positives.

[22] study investigates the deployment of AI-based intrusion detection systems (IDS) specifically for mobile networks. The research by [23] and colleagues addresses the challenges intrusion detection systems face, especially with the growing complexity of cyber threats. [24] work reviews a deep learning- based IDS developed for the Industrial Internet of Things (IIoT).

[25] paper discusses the application of machine learning techniques in IDS for 5G networks. The importance of explainable artificial intelligence (XAI) in intrusion detection is underscored by study [26] which assists security analysts in understanding and evaluating decisions made by complex Machine Learning-based IDS models. The research by [27] discusses the array of data attributes and types of attacks that can influence IDS efficiency, focusing on tailored performance metrics for evaluating IDS across different datasets. In [28] research delve into cutting-edge developments in machine learning (ML)-based intrusion detection, including self-learning models, federated learning, and integration with 5G and IoT networks. The study by [29] sheds light on Deep reinforcement learning-based IDS, optimizing the model's ability to adapt to changing network behaviors and autonomously adjust to new types of intrusions. In [30] research explores federated learning as a privacy-preserving approach in intrusion detection systems (IDS), allowing multiple entities to collaborate on improving model performance without sharing sensitive data.

III METHODOLOGY

Using a comparison technique, this review paper examines different machine learning (ML) algorithms utilized in intrusion detection systems (IDS) based on Machine Learning approaches.It examines important machine learning techniques including supervised, unsupervised and hybrid approaches evaluating how well

they identify anomalies and harmful activities. This evaluation provides feasibility study of each model for real time detection, idea drift, flexibility and scalability within network, recall and computing efficiency.

A. DATA COLLECTION AND FEATURE EXTRACTION

Finding peer reviewed publications and conference papers about machine learning techniques for intrusion detection systems (IDS) is a part of the data collection process for this review paper. The selection process uses relevance to machine learning IDS methodologies, publication dates from 2019 to 2024 and impact measures to filter studies. This procedure aims to ensure a comprehensive and current representation of developments in machine learning for IDS technology.

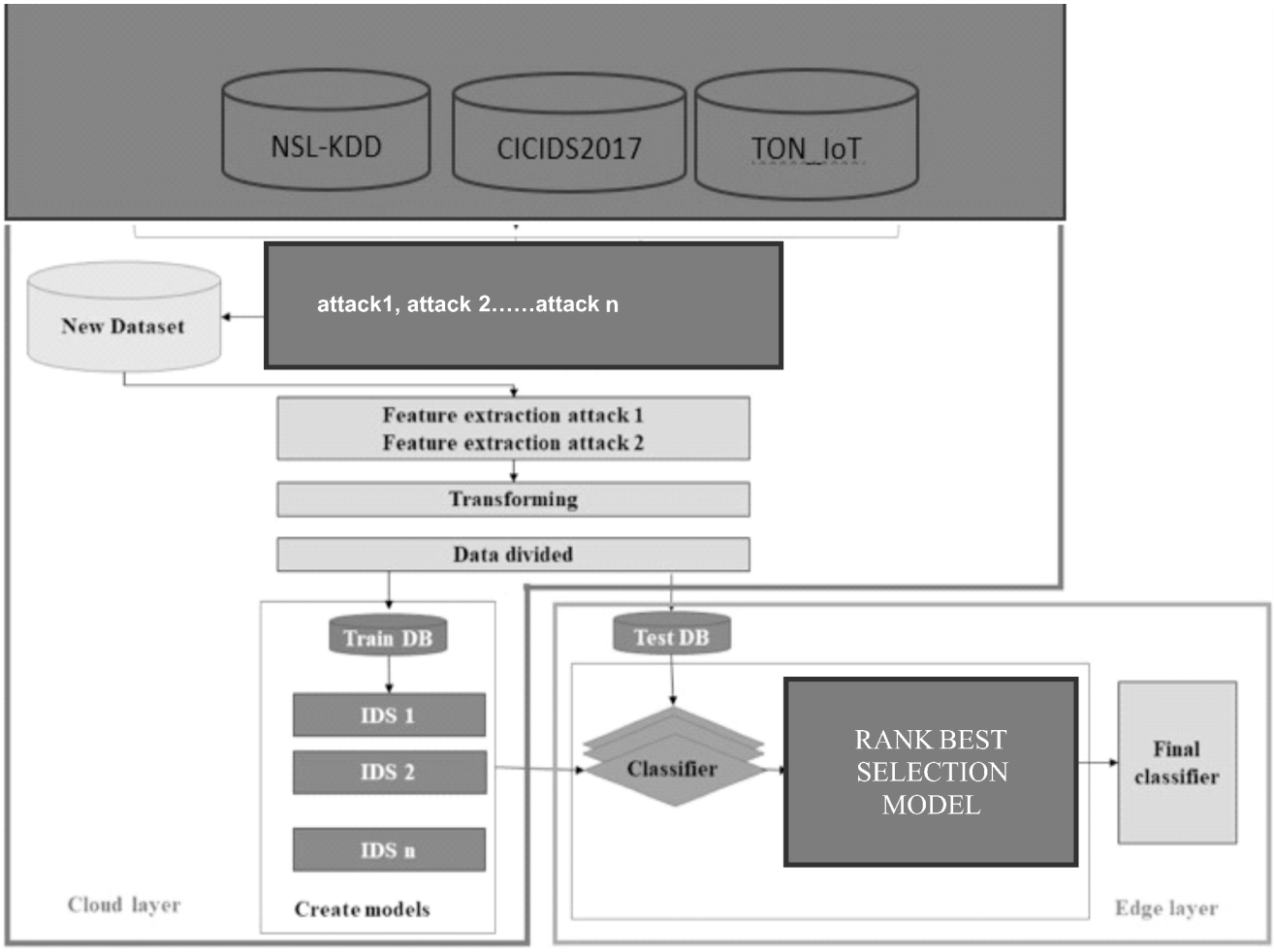

Figure 1 : Ids Architecture With Ml Integration

To ensure robust IDS model evaluation, researchers utilize various benchmark datasets.

Table 2: Overview of Datasets Used in the Study

Dataset	Year	Features	Attack Types	Application Domain
NSL-KDD	2009	41	DoS, U2R, R2L, Probe	Network IDS
CICIDS2017	2017	80+	DDoS, Brute Force	Real-time traffic

Feature selection methods play a crucial role in enhancing the efficiency and effectiveness of IDS models:

1. Principal Component Analysis (PCA) - Principal Component Analysis (PCA) converts high-dimensional data into a lower- dimensional space with most of the variation retained. The model performance is enhanced further by eliminating redundant features. PCA reduces dimensionality by transforming the dataset into a set of linearly uncorrelated principal components:

$$C = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(x_i - \bar{x})^T \quad \ldots\ldots\ldots\ldots\ldots (1)$$

where x_i represents the feature vectors, and $\bar{x}$ is the mean feature vector.

The principal components are obtained by solving:

$$c_v = \lambda_v \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

where λ are the eigen values and v are the corresponding eigenvectors.

2. Correlation-based feature selection - The most relevant features are retained by applying correlation-based feature selection, which identifies and removes highly correlated features. By reducing multicollinearity correlation-based feature selection enhances IDS model accuracy and interpretability. This method measures the correlation between input features and the target variable using the Pearson correlation coefficient:

$$r_{xy} = \frac{\sum(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum(x_i-\bar{x})^2 \sum(y_i-\bar{y})^2}} \quad \ldots\ldots\ldots\ldots\ldots (3)$$

where x_i and y_i are individual observations of features and the target variable.

3. Mutual Information- Mutual information measures how much the target variable depends on the input features. Features with a higher mutual information score are selected for model training since they give a larger contribution to intrusion detection. Identification of non-linear relationships among variables is facilitated by this method.

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \quad \ldots\ldots (4)$$

where $p(x,y)$ is the joint probability distribution of features x and target y

4. Recursive Feature Elimination (RFE)- In the dataset, all but the most important features remain due to the use of Recursive Feature Elimination (RFE), which has the effect of eliminating the less important features incrementally by examining model

performance. This method takes particular advantage when used with supervised learning models.

Using these feature selection approaches, IDS models can improve detection accuracy, minimize computational complexity and avoid over fitting. Constructing IDS models involves selecting relevant features and dataset quality. Dimensionality reduction and enhanced classification performance are often achieved using Principal Component Analysis (PCA), Mutual Information and Recursive Feature Elimination (RFE). As typical datasets for IDS testing, NSL-KDD and CICIDS2017 offer diverse attack scenarios for training and testing Machine Learning models.

B. CATEGORIZATION OF MACHINE LEARNING TECHNIQUES

Supervised learning, unsupervised learning and hybrid methods are the three main categories into which the reviewed literature divides machine learning techniques for intrusion detection systems. Due to the rapid increase in cyber threats, there has been a shift toward more complicated models like deep learning and federated learning. The quantity of papers, the variety of algorithms and application domains including cloud environments and Internet of Things are the main subjects of analysis. Studies compare the efficiency of each method by using performance criteria such as accuracy, precision, recall, F1-score and latency.

SUPERVISED LEARNING

Using labelled datasets, supervised learning approaches train intrusion detection systems (IDS) models to identify malicious or benign network traffic. Typical algorithms for supervised learning are:

- Support Vector Machines (SVM) -are computationally costly but effective with high-dimensional data.
- Decision trees (DT)- are quick and easy to understand, yet they might overfit.
- Random Forest (RF)-An ensemble of decision trees called Random Forest (RF) lowers variance and increases accuracy.
- Neural Networks (NN)- Deep learning models that can identify intricate attack patterns, but they demand a lot of processing power.

UNSUPERVISED LEARNING

Network traffic anomalies can be found using unsupervised learning techniques without the need for labelled data. Typical methods include of:

- Clustering (K-Means and DBSCAN)-Network traffic is grouped into clusters according to similarities.
- Autoencoders: Deep learning models that identify anomalies by identifying departures from typical traffic patterns.
- Isolation forests-An efficient tree-based technique for identifying outliers in high-dimensional datasets

ENSEMBLE LEARNING

Efforts directed at ensemble learning aim at advancing model robustness and accuracy by combing a range of models. This involves a number of techniques.

- Bagging (Random Forests)-Ensemble learning algorithms proceed to build a collection of learners and then employ them for training. Such trees can be built on different bootstrap versions of the training data set.
- Boosting (such as AdaBoost and XGBoost)- In this case, weaker sub-learners are integrated in order to obtain a stronger learner. It is based on the idea that we build learners one at a time, and each new learner tries to fix the mistakes that the right model did for your predictions.
- Stacking – This is the super advanced ensemble method where several machine learning models are combined and the final predictions are made by a meta-learner.

C. OPTIMIZATION TECHNIQUES FOR IDS MODELS

IDS Performance enhancements through optimization strategies goes hand in hand using the following techniques-

1. Hyperparameter Tuning-As part of model optimisation, model parameters can be fine-tuned such that performance significantly improve. Methods commonly include:

- Grid Search: Over a specified value of the hyper parameters.
- Random Search: Best hyper parametric set is achieved by choosing random.
- Bayesian Optimisation: Maximizing the rate of performance using some probability models.

2. Cross-Validation

Cross-validation guarantee dependable model performance and avoids overfitting. Principal techniques include:

- K-Fold Cross-Validation: Disintegrates the data into K parts and trains the model on different configurations.
- Stratified Cross-Validation: It guarantees that there is no imbalance in the class distribution in the training and validation sets.

3. Dropout Regularization

Dropout is applied to deep learning structures to ensure that there is no over fitting by turning off a certain random percentage of all neurons during their operation. It is also one way of making generalized and robust models.

D. EVALUATION OF MODEL EFFECTIVENESS

To assess the effectiveness of the model in various machine learning based intrusion detection systems key performance indicators are measured and analyzed. Accuracy measures the ability to correctly identify malicious and benign traffic. Recall assesses the model's sensitivity to actual intrusions which is crucial for reducing false negatives. Precision concentrates on the true positive rate among identified intrusions. For datasets with class imbalances the F1-Scoreoffers a balanced perspective of model performance by combining precision and recall. Latency assesses the capacity for real-time processing which is crucial for systems that need to react quickly to threats.

TABLE II. PERFORMANCE METRICS OF ML MODELS IN IDS

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Latency (ms)
Supervised Learning	85	83	80	81	20
Unsupervised Learning	78	75	70	72	15
Hybrid/Ensembe Models	90	88	85	86	25

IV. CHALLENGES IN ML-BASED IDS

Optimising model performance while maintaining scalable and real-time threat detection is the first challenge in Machine Learning based intrusion detection systems. Effective model training is hampered by the challenges associated with feature selection in high-dimensional datasets. Attack samples that are under-represented due to class imbalance may result in low detection rates for uncommon but serious threats. Another serious challenge faced by machine learning based intrusion detection system is false positives and such incorrect classifications might result in pointless warnings that hinder security efforts. Scalability is also a major concern since large- scale network settings require adaptable and resource-efficient machine learning models to manage growing traffic volumes without sacrificing performance.

V CONCLUSION AND FUTURE RECOMMENDATIONS

This paper emphasizes the significant advancements and trends in machine learning-based intrusion detection systems underscoring their growing relevance in addressing complex and evolving cyber security threats. The investigation demonstrates the effectiveness of various machine learning techniques ranging from traditional supervised methods to more sophisticated hybrid and ensemble approaches. These techniques offer enhanced accuracy, flexibility and scalability for real-time intrusion detection systems. It is discovered that cloud-based and edge computing solutions are crucial for managing environments with high traffic and limited resources, which makes IDS more flexible to meet the needs of contemporary networks. Additionally, it is clear how crucial it is to pick and assess a variety of datasets in order to provide robust model evaluation and guarantee generalizability across real-world applications. Overall, advancements in computational infrastructure and ongoing ML algorithm development promise to substantially bolster IDS capabilities, making them indispensable in today's cyber security landscape. According to the analysis deep learning models such as recurrent and convolutional neural networks are becoming more and more well-liked in IDS because to their accuracy and versatility. However, in situations with limited resources such as in the case of Internet of Things their high computing demand presents deployment issues. For lightweight Intrusion Detection

System applications conventional machine learning methods like decision trees and support vector machines are still applicable. The rise of hybrid and ensemble methods which merge the strengths of multiple models to enhance detection precision while addressing concept drift and evolving network threats represents a significant trend. As machine learning based Intrusion Detection System models became more advanced, they have overcome the drawbacks of traditional methods by enhancing processing speed, accuracy and adaptability. However, challenges remain in the areas of datasets availability and standardization particularly for emerging fields such as IoT and 5G. Future directions include integration of federated learning for privacy-preserving Intrusion Detection System and exploration of explainable Artificial Intelligence to enhance system transparency and trust.

1. Explainable Artificial Intelligence (XAI) For Intrusion Detection Systems-Explainable Artificial Intelligence (XAI), which has emerged in the recent trends, is essentially responsible for designing ML-based Intrusion Detection Systems that are human dignifying in nature, as it is the case the norm. Such

technologies are useful as will be best explained further in this part are. With this, it can be quite hard explaining to a security analyst how a particular attack has been caught as in many traditional ML or deep learning models operate as black boxes and are therefore near impossible to trace. There are numerous methods of XAI applications obtainable today including; SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) which can be applied to explain the reasons for a machine's decision. As a result, this explains why greater trust, responsibility, and the ability to debug have security systems in relation to malicious threats. In Progressing IDS technologies such as these vulnerable technologies it will be obligatory to introduce XAI for the purpose of improved clarity in decision making, compliance as well as the trust of the end user.

2. Privacy-Preserving Federated Learning: Federated learning allows for training an intrusion detection system in a coordinated manner without putting data confidentiality at risk. It would be our recommendation to implement optimized federated learning in the design and structure of IDS in upcoming systems more so in protected areas.

3. Edge and Cloud-Based Intrusion Detection Systems Put up an IDS at the edge destination will reduce detection latency and make the threat retaliation in real-time a reality. Management of cloud-based IDS solutions will require the employment of real time machine learning solutions.

4. Adaptive Learning with Reinforcement Learning Reinforcement learning is incorporated in the IDS systems, it would enhance self-optimizing toward the changing cyber space. Such predictive systems can automatically upgrade detection mechanisms upon scanning all new attacks.

5. Development of Comprehensive Benchmark Datasets Tangible inputs as benchmarks must be quantified for future intrusion detection system research. More specifically such benchmarks should also be supplemented by standardization of data for the training of models in diverse networks in future attempts of evaluations.

The ongoing advancements in hardware such as edge computing also present promising avenues for deploying these sophisticated IDS models in diverse and real- world settings. The advancementof federated learning, particularly for privacy-sensitive contexts like IoT and 5G where centralized data storage is not feasible represents a significant direction for the development of Machine language-based Intrusion Detection Systems (IDS). It is important to integrate adaptive learning features that enable the IDS to respond to new attack vectors in real time, especially through reinforcement learning. Researching lightweight, efficient models suitable for edge computing is very essential to guarantee performance in limited-resource settings. Lastly, the creation of definitive benchmarks and varied datasets is imperative for consistent and dependable evaluations and thus boosting the effectiveness of IDS under various network scenarios.

REFERENCES

[1] Ghani, A. A. A., Abdullah, A., & Hakim, F. (2021). An IDS for IoT using machine learning. MDPI.

[2] Khan, F. A., & Gumaei, A. (2019). Machine learning classifiers for intrusion detection. Springer.

[3] Thamilarasu, G., & Chawla, S. (2020). Anomaly detection for IoT using DBNs. IEEE Xplore.

[4] Sandeep, G., et al. (2020). Sparse autoencoders for IDS. IEEE Xplore.

[5] da Costa, K. A. P., et al. (2021). Hybrid IDS models in IoT. Cyber security .Journal.

[6] Yang, X., et al. (2019). Modified clustering for IDS. arXiv.

[7] Gupta, M., et al. (2022). Advances in deep learning-based IDS. IEEE Xplore.

[8] Ali, R., & Singh, S. (2023). Federated learning approaches for IDS. Springer.

[9] Sharma, A., et al. (2024). Ensemble learning for network intrusion detection. IEEE Transactions on Cybernetics.

[10] Oprea, M., et al. (2021). A survey on evolving IDS and concept drift handling. Frontiers in Computer Science.

[11] Patel, N., & Joshi, A. (2022). Real-time IDS with deep learning. Journal of Network Security.

[12] Pande, A., & Chauhan, R. (2023). Scalable IDS using cloud-based ML. MDPI.

[13] Li, Y., et al. (2019). A comparative study of ML algorithms in IDS. IEEE Access.

[14] Wang, J., & Zhang, Q. (2020). Security-aware IDS using autoencoders. Symmetry.

[15] Malik, S., et al. (2021). Survey on supervised IDS methods. Springer.

[16] Acharya, B., et al. (2022). Resource-efficient IDS in edge computing. IEEE Internet of Things Journal.

[17] Han, T., & Liu, F. (2020). Benchmarking datasets for IDS. Journal of Big Data.

[18] Park, J., & Kim, H. (2023). Hybrid intrusion detection for smart grids.Energy Informatics.

[19] Bansal, R., et al. (2022). Anomaly-based IDS using GANs. IEEE Access

[20] Xiao, Y., et al. (2021). IDS with feature reduction techniques. Journal of Cybersecurity.

[21] Singh, P., & Kumar, S. (2023). Comparative analysis of anomaly detectors. Computer Networks.

[22] Rana, A., et al. (2024). AI-based IDS for mobile networks. Springer.

[23] Farooq, A., et al. (2019). Review on IDS challenges and solutions. IEEE Xplore.

[24] Desai, K., & Vora, M. (2020). IDS for industrial IoT using deep learning. MDPI.

[25] Haque, T., & Rahman, M. (2022). Real-time intrusion detection in 5G. Journal of Network Security.

[26] Roy, D., et al. (2023). Explainable AI in IDS. IEEE Transactions on Cybernetics.

[27] Ahmed, F., & Hussain, Z. (2021). Dataset-specific IDS performance metrics. Journal of Computer Science.

[28] Zhao, J., et al. (2024). Future trends in ML-based IDS. IEEE Access.

[29] Neupane, K., & Shrestha, P. (2019). IDS with deep reinforcement learning. Journal of Cyber security.

[30] Joshi, A., & Patel, R. (2023). Federated IDS with privacy- preserving techniques. IEEE Access

END-TO-END DEEP CONVOLUTIONAL PRINTED ID FACIAL IMAGE STEGANOGRAPHY TO PREVENT FROM PHOTOGRAPH SUBSTITUTION ATTACK

Kiruthika N[1], Nandhini GS*[2]

ABSTRACT

At the point when we discuss a "character card," we're alluding to a proper picture ID that, in Germany, can be utilized thusly. Among the most famous purposes for savvy cards are government-supported retirement cards, electronic IDs, electronic markings, common cards, key cards for getting to safeguarded regions or authoritative designs, and smart excursion documents. Various safeguards are contained in these records. Battle the act of manufacturing reports. Considering that these security highlights are challenging to move beyond, criminal assaults against character affirmation frameworks as of now depend on incorrectly getting real files and changing facial pictures. Any helpful development should have a construction of convincing characters. To lessen the probability of coercion, these state-run organizations and character makers ought to ceaselessly refresh and improve their security conventions. Subsequently, the essential functional steganography strategy explicitly intended for the photographs ordinarily found on customary ID cards is the convey StegoCard. StegoCard is a state of the art facial picture steganography model made to securely and imperceptibly embed secret messages into photographs of individuals. A Significant Convolutional Autoencoder (PCAE), which speeds up the encoding and disentangling tasks, is at the core of this model. The PCAE integrates the mystery message into its inactive portrayal after first dissecting the information facial picture's credits. Through this coordination, the message is unpretentiously concealed inside the design of the Stego picture, an apparently indistinguishable rendition of the first.

Keywords: Facial Image Steganography, Identity Verification Security, Profound Convolutional Autoencoder (PCAE), Anti-Fraud Protocols, Smart ID Card Technology.

I. INTRODUCTION

Any record that can be utilized to demonstrate somebody's character is called an ID report (otherwise called a piece of personality or ID, or essentially papers). It can likewise be known as a visa card, distinguishing proof card (IC, ID card, or resident card), or a short, nonexclusive FICO rating card length.[b] While certain nations may likewise request recognize confirmation utilizing casual or close personality records, others might have formal ID documents, for example, public character playing a game of cards, which can be compulsory or discretionary. A character report that incorporates an individual's photograph might be called a picture ID. For ID confirmation, a driver's permit can be conventional in numerous nations in the event that a proper ID report isn't given. A few nations never again acknowledge driver's licenses as recognizable proof, as a rule since they are obsolete or effortlessly distorted in such nations and never again terminate as records.

Most of nations acknowledge international IDs as a type of distinguishing proof. In specific nations, everybody should have a personality report accessible consistently. Numerous nations require all outsiders to have an identification from their nation of origin, or periodically a cross country character card, which can be gotten without warning in the event that they never again have one. have a home that is allowed inside the US. The reason for the distinguishing proof report is to connect an individual to character measurements, typically tracked down in a data set. The person is joined to the report utilizing the picture and the proprietor's data. The recognizable proof report's non-public insights gift, alongside the carrier's complete name, age, begin date, home, character number, card number, orientation, citizenship, and the sky is the limit from there,

Department of Computer Science and Engineering [1]
Karpagam Academy of Higher Education, Coimbatore, India[1]
snkiruthikasri6@gmail.com[1]
Department of Computer Science[2],
Sri Shakti Institute of Engineering, Coimbatore[2]
nandhinicse@siet.ac.in[2]

* Corresponding Author

are the primary factors that interface the ID report and measurements information base. The most dependable strategy is to have a careful public character number, but a few nations don't have these or do exclude them in their distinguishing proof records.

Right now, it is feasible to communicate something specific that is noticeable to both the carrier and the typical beneficiary by inserting it inside a photograph or message. As per steganography, information can be furtively covered and afterward uncovered when required. The maxim "stego-picture" signifies the real picture after it has been hidden, while the precept "cover picture" recommends a fake picture. To prevent busybodies from deciphering a mystery message, cryptography encodes it. In this methodology, consolidating steganography and encryption adds one more level of security. We had the option to expand the secret of the message while diminishing its file size by utilizing picture pressure.

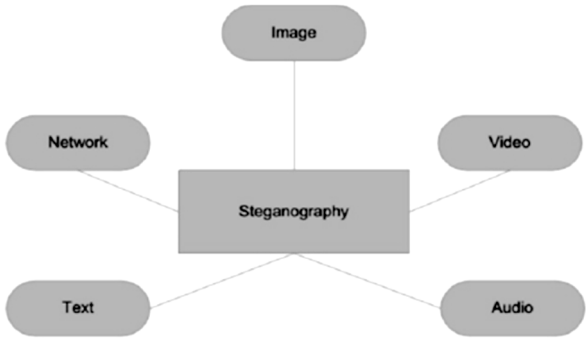

Figure 1: Steganography

Steganography is a famous type of encryption where a mystery message is taken cover behind a picture. Since current pictures are so broadly accessible on the web, they are sporadically utilized as cover objects. This is because of the way that they offer an adequate amount of pixels that can be utilized to conceal specific data without compromising the picture's general tasteful allure. Starting with the technique for disguising data inside the most un-fundamental pieces of the picture (LSBs), picture steganography has advanced to additional perplexing strategies like material adaptable steganography, which successfully changes installing costs for each cover pixel utilizing a mutilation limit. The presentation of a cover picture is accomplished by restricting a turning limit. In an open construction circumstance, it is critical to conceal the dispatch's present and genuine states from unapproved beneficiaries to work on the security of undercover dispatches. It is known as the "examination of covered up or secret correspondence".

For any steganographic procedure to be viewed as effective, it should fulfill the three standards of liberality, cutoff, and straightforwardness. Constraints are the most touchy data that can be dealt with in a record. On the off chance that the data on the cover and the stego records are almost something very similar, the steganographic technique is absolutely protected and immaterial. The Stego report ought, taking everything into account, areas of strength for have since it can get through numerous assaults yet uncover the covered up message with minimal information loss.

A. Auto encoder

A fake brain network planned for include extraction and solo learning is known as a Profound Auto Encoder. Its parts incorporate an encoder that converts input information into a lower-layered, minimal portrayal. "Profound" portrays the encoder's few layers, which permit the model to recognize unpredictable, various leveled designs in the information. The encoder removes logically dynamic data from crude info information by handling it through a grouping of stowed away layers. To find complex information connections, these layers generally utilize non-direct enactment capabilities like sigmoid or ReLU. Information's dimensionality diminishes as it travels through these layers, delivering a compacted encoding. Reproduction mistake between the information and the encoded yield should be limited while preparing a Profound Auto Encoder. The nature of the encoded portrayal is improved by altering the organization's loads and inclinations utilizing techniques like slope plunge and back propagation. Through this strategy, the model can independently learn huge examples. Peculiarity recognition, information denoising, and dimensionality decrease are among the undertakings that Profound Auto Encoders succeed at. They are utilized in spaces like PC vision, where

they assist with picture reproduction and element extraction, and in signal handling and normal language handling, where they support errands like discourse acknowledgment and text examination.

B. Steganography

Steganography is the most common way of disguising data inside one more message or actual thing to stay away from location. Steganography can be utilized to conceal practically any kind of computerized content, including text, photographs, motion pictures, and sound. The secret information is then revealed at its objective. Steganographically covered information is once in a while scrambled prior to being disguised in an alternate sort of record. On the off chance that it isn't encoded, it could be taken care of such that makes it harder to find.

As a technique for secret correspondence, steganography is once in a while contrasted with cryptography. Nonetheless, steganography needn't bother with that information be encoded before to transmission or unscrambled utilizing a key upon appearance, so the two are not compatible.

II. LITERATURE REVIEW

Computerized steganography involves the host sign to conceal data in a manner that isn't noticeable to the watcher. The discrete wavelet change, which changes numbers to numbers, takes into consideration a full replication of the first picture. Thusly, we propose a strategy that incorporates the sign piece stream into the LSBs of the certifiable picture's whole number wavelets. To fix immersion pixel parts and recuperate the encoded messages without losing them, the methodology additionally preprocesses the cover picture. Due to our rising dependence on computerized media, There is a quick requirement for imaginative ways of safeguarding it from unapproved use. One procedure that has been used for quite a while in reasonable applications is encryption. The essential help that cryptography offers is the ability to move information between people in a way that forestalls unapproved access. Trial results showed the wonderful straightforwardness of the proposed approach even with huge message sizes.

The method involved with sending information by means of an actual media from its source to its objective is known as information transmission. Coaxial link and curved pair wires are utilized in systems administration to move information starting with one area then onto the next. These information specialized strategies are more slow in nature, and there is no information assurance. Furthermore, information might release or be lost during transmission. We utilize fiber optics to get around these transmission issues. Information spillage is more outlandish in fiber optics since the information is sent as light shafts. Moreover, it utilizes a couple of safety efforts to guarantee safe information move. Prior to being shipped off the objective as light, the information should initially be encoded radiates. We utilized pictures to add encryption into fiber optics in our recommended approach. Furthermore, various encryption calculations have been proposed to make optical medium information secure, helpless, and to address security issues and difficulties. AES, DES, and RSA calculations have been contrasted all together with decide the best security calculation that ought to be utilized in optical medium to make it secure and impervious by programmers.

The framework of the web has progressed essentially contrasted with conventional ways. Therefore, patients' very classified clinical records need additional consideration and security. We have made a superior technique to expand the subtlety and information concealing capability of steganographic pictures. The specialty of concealing data and a procedure to cause it to seem like it isn't installed is called steganography. Contrasted with encryption, which simply covers the letter's substance and not its presence, it is a more powerful correspondence security method. To guarantee that any changes to the payload are imperceptible, the first message is concealed inside a transporter. This article will examine how computerized pictures can be utilized as a transporter to disguise messages. Besides, the viability of a few steganography instruments is explored. in this review. Steganography is a valuable instrument for sending restricted information across a correspondence medium. The transporter picture and secret picture are joined to make the hidden imaging. Without recovery, it is challenging to find the covered up photographs.

The most common way of sending information through an actual media from its source to its objective is known as information transmission. Coaxial link and contorted pair wires are utilized in systems administration to move information starting with one area then onto the next. These information specialized techniques are more slow in nature, and there is no information assurance. Furthermore, information might release or be lost during transmission. We utilize fiber optics to get around these transmission issues. Information spillage is more uncertain in fiber optics since the information is sent as light bars. Furthermore, it utilizes a couple of safety efforts to guarantee safe information move. Prior to being shipped off the objective as light, the information should initially be encoded. radiates. We utilized pictures to add encryption into fiber optics in our proposed approach. Furthermore, various encryption calculations have been proposed to make optical medium information secure, helpless, and to address security issues and difficulties. AES, DES, and RSA calculations have been contrasted all together with decide the best security calculation that ought to be utilized in optical medium to make it secure and impervious by programmers.

Information stowing away has drawn a ton of interest of late since it goes about as a choice to get transmission. A mysterious material is typified with an image utilizing an assortment of picture exemplification methods, like the Most un-Critical Piece (LSB) replacement. The uniqueness and nature of the substance exemplification would be difficult to guarantee. Every one of the picture's red, green, and blue layer blocks has gone through a scrambling cycle utilizing the Sudoku plot in the proposed article. The picture layers would be isolated into blocks, and remarkable scrambling methods would be applied all through the blocks to deliver the scrambling picture. The muddled picture was then uncovered by applying the Sovereign Visit crossing design from the chess game and the standard LSB replacement approach. to the epitome of the secret stream. Following the consummation of the implanting system, the muddled picture will be isolated into blocks, and the blocks will go through exact descrambling to recover the stego picture — the picture that most intently looks like the first. The stego picture is separated into blocks on the getting side so the pertinent blocks can be exactly mixed to recuperate the mystery stream utilizing the Sovereign visit design. The expected system is found to have a lower probability of being exceptionally prescient and having interesting examples after the tests.

III. METHODOLOGY

StegoFace's execution approach is a calculated two-step technique that utilizes facial picture steganography to encode stowed away information in photos of individuals. Information securing by means of information gadgets is the underlying stage, during which facial photos are taken from ID or MRTD reports. The stenographic system depends on these photos. To securely incorporate mystery messages into the picture without forfeiting its planned capability for confirmation or influencing its visual quality, the subsequent stage is handling the face picture utilizing an encoder.

To ensure that the secret information is imperceptible and save the picture's uprightness for routine personality and travel record check, the encoder utilizes refined steganography calculations. This method utilizes calculations that are enhanced for incredible security and little twisting, ensuring that encoded information is impervious to unapproved evacuation or change. The methodology utilized by StegoFace ensures that unrivaled insurance and secure interchanges are incorporated directly into ID and MRTD frameworks. By giving a secret layer, safeguarding basic information, and frustrating wholesale fraud, this strategy further develops security.

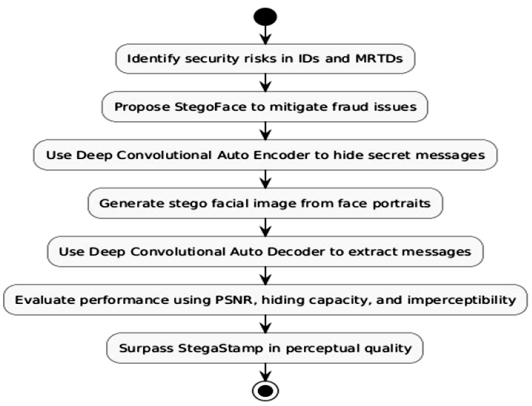

Figure 2: Architecture diagram

A. Proposed Methodology

The proposed framework, Stego Face, is a state of the art innovation that utilizations face photos to encode secret correspondences to work on the security of ID (ID) and machine-discernible travel records (MRTDs). In light of the rising interest for imaginative ways of safeguarding delicate information and stop report extortion, Stego Face is the main model to be economically delivered explicitly as a record security approach. Stego Face depends on the utilization of facial picture steganography, which makes it conceivable to consolidate privileged information in facial representations without forfeiting the picture's stylish allure or handiness for confirmation. This inventive technique saves the respectability of ID archives while ensuring secure association.

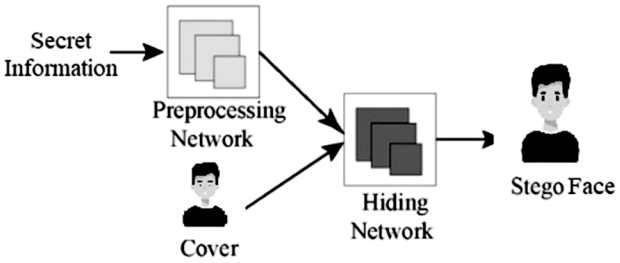

Figure 3: Stego face

Stego Face utilizes info and result gadgets (encoders) in a two-step, organized technique. To coordinate secret messages into the face picture, the encoder processes the information. Conventional ID and travel papers can be additionally gotten by utilizing these encoded photographs in secure distinguishing proof frameworks. We are very glad to have been quick to present Stego Face, a progressive innovation for further developing record security. It is a vital part of contemporary report security strategies due to its possible purposes, which incorporate secure interchanges and character confirmation.

B. Encoding Mechanism (Encoder)

One fundamental piece of the Stego Face framework that implants stowed away messages into preprocessed face photographs is the encoding strategy. This stage utilizes progressed steganography methods, which permit privileged intel to be covered by making simply minor acclimations to the facial picture's pixel information. The goal is to save the picture's respectability for impending investigation or acknowledgment errands while ensuring that these progressions are imperceptible to the natural eye. At the point when a face picture has been preprocessed, it is shipped off the encoder, which utilizations modern calculations to embed the mystery message into the picture. These calculations are expected to ensure that the encoding method doesn't modify the presence of the facial picture or impede facial acknowledgment frameworks' ability to distinguish it. Profound Convolutional Auto encoders, which are procedures in view of AI customized for encoding position, are one frequently utilized approach. Profound brain networks are utilized in these auto encoders, which are prepared to become familiar with a consolidated portrayal of the information while keeping up with significant visual subtleties and easily coordinating the secret message. Steganography techniques are utilized in the process to roll out little improvements to the picture's pixel values. An unassisted spectator wouldn't have the option to recognize these progressions since they are made purposely to try not to perceptibly affect the picture's visual attributes. This empowers the encoded picture to convey implanted information while protecting its unique design.

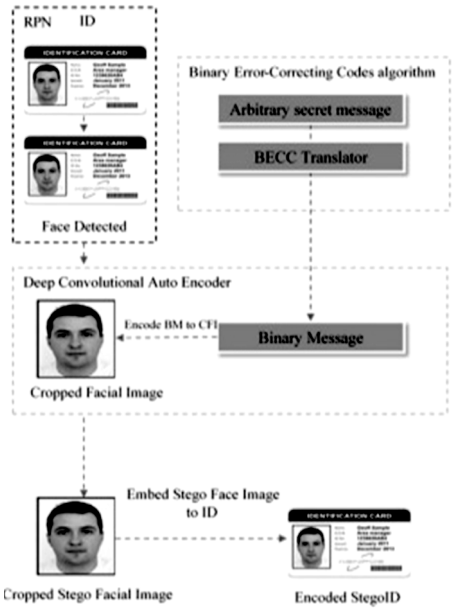

Figure 4: Image encoder

With regards to inserting messages, AI based encoding procedures like convolutional auto encoders or other brain designs can give upgraded adaptability, flexibility, and productivity. These techniques utilize brain organizations' learning abilities to amplify the disguise of data, bringing down the chance of discovery and ensuring versatility under different visual circumstances. By safely coordinating secret data while keeping up with the picture's regular appearance and characteristics, the encoding instrument basically goes about as a connection between information stowing away and facial picture handling. This imaginative strategy guarantees effective information disguising without forfeiting framework proficiency, protection, or security by using state of the art encoding procedures.

C. Steganographic Integration

A critical stage in the Stego Face framework is the steganographic combination strategy, which securely integrates secret messages into facial photographs without undermining their tasteful allure or capacity to be utilized for biometric validation and confirmation. This stage keeps up with the first facial picture's helpfulness as a biometric distinguishing proof while ensuring that the secret data stays stowed away yet open for the ideal purposes. Contingent upon the objectives and necessities of the framework, steganographic coordination involves modern methods that can work in either the recurrence area or the spatial space. Spatial space approaches are a famous method for embedding a disguised message into a facial picture. By straightforwardly changing the pixel esteems, these strategies make minor acclimations to specific region of the picture without making any undeniable visual irregularities. Since they just change the most un-huge pieces of pixel values, procedures like Least Critical Piece (LSB) addition are every now and again utilized in spatial space steganography. This ensures that the hid message is inserted with minimal measure of unsettling influence to the picture's visual characteristics. Applications where speedy and productive message inserting is critical can profit from the spatial area's usability and figuring effectiveness.

Be that as it may, by implanting data in the change space rather than straightforwardly in pixel values, recurrence area approaches give another option. Utilizing procedures, for example, the Discrete Fourier Change (DFT), Discrete Cosine Change (DCT), or other sign handling draws near, these strategies involve changing over the picture into an unmistakable numerical portrayal. Once in the changed space, the picture's recurrence coefficients are delicately modified to consolidate the hid data. This strategy enjoys the benefit of being stronger to commotion and pressure, protecting the trustworthiness of the secret message even in different situations. In circumstances where an elevated degree of protection from altering or debasement is fundamental, recurrence space advances are much of the time utilized. Various reasons impact the choice among spatial and recurrence space draws near, including the fundamental level of computational productivity, versatility, and impalpability. The goal is consistently something very similar, no matter what the strategy: to ensure that the hid message is securely and easily integrated into the image while protecting the first face information's visual quality. Since steganographic joining should keep up with the facial picture's helpfulness for biometric check and validation, it is particularly vital in biometric settings. For exact recognizable proof, facial acknowledgment frameworks require solid, great photographs. Steganographic strategies should hence ensure that the biometric attributes fundamental for matching methodology are neither misshaped or crumbled during encoding. Biometric frameworks can in any case perceive and handle the picture since the progressions made during coordination are slight to such an extent that they are not perceptible to the natural eye.

IV. RESULT AND DISCUSSION

By integrating face picture steganography into recognizable proof (ID) and machine-decipherable travel reports (MRTDs), the recommended arrangement, StegoFace, represents a progressive way to deal with record security. The discoveries show that StegoFace effectively integrates covered data into facial representations while keeping up with the visual allure and helpfulness of the

picture for approval. This double capacity adds serious areas of strength for a for safe information encoding while at the same time ensuring the framework's consistence with current security systems. StegoFace is a strategy for safely imparting by encoding messages utilizing input gadgets. The aftereffects of exploratory preliminaries show that encoded pictures keep up with both their utilitarian and tasteful respectability, making them impervious to assessment all through confirmation processes.

Table 1: Performance Comparison of Deep Autoencoder (DAE) and Logistic Regression (Baseline)

Metric	Deep Autoencoder (DAE)	Logistic Regression (Baseline)
Accuracy (%)	92.5	84.3
F1 Score	0.91	0.78
Recall	0.90	0.75
Precision	0.93	0.81

Stego Face's flexibility gives a mystery layer of security to basic information, making it particularly helpful in the battle against record extortion. Moreover, the capability of the innovation goes past ID. check to get correspondences applications, giving an adaptable answer for organizations overseeing significant information. Stego Face settles a critical defect in report security procedures by coordinating security at the picture level. Future advancements could expand its adequacy, opening the entryway for more extensive use in areas that request solid data security norms.

Figure 5: Output image

V. CONCLUSION

Stego Face is a progressive improvement in the field of report security that utilizes facial picture steganography to incorporate privileged data into Machine-Decipherable Travel Records (MRTDs) and ID records. This arrangement satisfies the earnest need for state of the art shields to forestall archive misrepresentation and safeguard delicate information by saving the tasteful trustworthiness of facial pictures while encoding secret interchanges. As the first economically accessible model explicitly intended for record security, Stego Face is an exploring strategy that joins information security with smooth convenience in confirmation systems.

To guarantee that the encoded yields are outwardly indistinguishable from the source photographs, the framework utilizes an encoder to embed stowed away messages into facial photos in a two-step methodology. This original methodology expands the potential for secure interchanges while reinforcing the security of regular distinguishing techniques. With potential purposes going from scrambled correspondences to personality check, Stego Face cements its situation as a critical part of contemporary security strategies. By sending off this creative apparatus, we accomplished a significant achievement in the improvement of secure recognizable proof innovations and laid out another benchmark for safeguarding the mystery and credibility of ID reports.

REFERENCES

[1] Ferreira, E. Nowroozi, and M. Barni, "VIPPrint: Validating artificial photograph detection and supply linking techniques on a large-scale dataset of published documents," J. Imag., vol. 7, no. 3, p. 50, Mar. 2021.

[2] Bazarevsky, Y. Kartynnik, A. Vakunov, K. Raveendran, and M. Grundmann, "BlazeFace: Sub-millisecond neural face detection on cellular GPUs," 2019, arXiv:1907.05047.

[3] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. IEEE/CVF Conf. Comput. Vis.

Pattern Recognit. (CVPR), Jun. 2019, pp. 4685–4694.

[4] R. L. Jones, Y. Wu, D. Bi, and R. A. Eckel, "Line phase code for embedding information," U.S. Patent App. sixteen 236 969, Jul. 4, 2019. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] S. Ciftci, A. O. Akyuz, and T. Ebrahimi, “A Reliable and Reversible Image Privacy Protection Based on False Colors,” IEEE Transactions on Multimedia, vol. 20, no. 1, pp. 68–81, 2018.

[6] M. Jiménez Rodríguez, C. E. Padilla Leyferman, J. C. Estrada Gutiérrez, M. G. González Novoa, H. Gómez Rodríguez, and O. Flores Siordia, “Steganography implemented withinside the beginning declare of images captured with the aid of using drones primarily based totally on chaos,” Ingeniería e Investigación, vol. 38, no. 2, pp. 61–69, 2018.

[7] L.-C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, "DeepLab: Semantic photograph segmentation with deep convolutional nets, atrous convolution, and completely related CRFs," IEEE Trans. Pattern Anal. Mach. Intell., vol. 40, no. 4, pp. 834–848, Apr. 2018.

[8] Ü. Çavusoglu, S. Kaçar, I. Pehlivan, and A. Zengin, “Secure photograph encryption set of rules layout the use of a unique chaos-primarily based totally S-Box,” Chaos, Solitons & Fractals, vol. 95, pp. 92–101, 2017.

[9] Z. Parvin, H. Seyedarabi, and M. Shamsi, “A new steady and touchy photograph encryption scheme primarily based totally on new substitution with chaotic function,” Multimedia Tools and Applications, vol. 75, no. 17, pp. 10631–10648, 2016.

[10] M. Khan and T. Shah, “An green chaotic photograph encryption scheme,” Neural Computing and Applications, vol. 26, no. 5, pp. 1137–1148, 2015

[11] Wu, Jiaxuan, et al. "Generative text steganography with large language model." Proceedings of the 32nd ACM International Conference on Multimedia. 2024.

[12] Li, Guobiao, et al. "Steganography of steganographic networks." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 37. No. 4. 2023.

[13] Zhou, Zhili, et al. "Generative steganography via auto-generation of semantic object contours." IEEE Transactions on Information Forensics and Security 18 (2023): 2751-2765.

[14] Mandal, Pratap Chandra, et al. "Digital image steganography: A literature survey." Information sciences 609 (2022): 1451-1488.

[15] Rathore, Manjari Singh, et al. "A novel trust-based security and privacy model for internet of vehicles using encryption and steganography." Computers and Electrical Engineering 102 (2022): 108205.

[16] Liu, Minglin, et al. "Adversarial steganography embedding via stego generation and selection." IEEE Transactions on Dependable and Secure Computing 20.3 (2022): 2375-2389.

[17] Almomani, Iman, Aala Alkhayer, and Walid El-Shafai. "A crypto-steganography approach for hiding ransomware within HEVC streams in android IoT devices." Sensors 22.6 (2022): 2281.

[18] Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." Information Security Journal: A Global Perspective 30.2 (2021): 63-87.

[19] Megías, David, Wojciech Mazurczyk, and Minoru Kuribayashi. "Data hiding and its applications: Digital watermarking and steganography." Applied Sciences 11.22 (2021): 10928.

[20] Evsutin, Oleg, Anna Melman, and Roman Meshcheryakov. "Digital steganography and watermarking for digital images: A review of current research directions." IEEE Access 8 (2020): 166589-166611.