International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

An Enhanced Security Model for Protecting Data Transmission and Communication in Recent IoT Integrated Healthcare Industry Using Machine Learning Algorithm

Sriram Parabrahmachari[1], Srinivasan Narayanasamy[2]
[1]Sathyabama Institute of Science And Technology :Department of Computer Science and Engineering
Chennai, India.
e-mail: sri.chari2022@gmail.com
[2]Rajalakshmi Engineering College : Department of Computer science and Enigineering
Chennai, India.
e-mail: srinivasan.n@rajalakshmi.edu.in

Abstract— Different kinds of security need to be applied to various application-centric IoT networks. Safety is one of the most important aspects to be considered regarding user, device, and data. The healthcare industry is a special IoT network fully connected with medical/healthcare IoT devices. The data generated from the IoT devices are transmitted or shared from one hospital to another through the Internet. Healthcare data has more private, medical, and insurance information that intruders can use on the Internet. The intruders misbehave with the patient or the general public registered in the healthcare industry. Some intruders blackmail the patient based on their private/personal information. Healthcare industries and their research team are trying to create a security framework to safeguard the data to avoid these malicious activities. This paper aims to secure and analyze healthcare IoT data using the Support Vector Machine algorithm. It learns the entire dataset, classifies it, and calls the encryption-decryption algorithms (RSA) to secure private data. The proposed SVM and the RSA algorithm are implemented in Python, and the results are verified. The performance of the proposed SVM-RSA is evaluated by comparing its results with the other algorithms..

Keywords- Internet of Things, Device Security, Data Security, Healthcare Security, IoT-Security.

I. INTRODUCTION

The Healthcare sector is one of the largest sectors in India. The economy and employment level of India is rising based on healthcare industries. It includes medical equipment manufacturing, drug production, caretaking, hospital, telemedicine, and health insurance. The major role of the healthcare industry is to strengthen every individual's life. Recently, many types of machinery have been used in hospitals to analyze and diagnose patients' health conditions. But the machinery consumes more time to diagnose and predict the result and is more expensive. It affects both the doctor and the patients. Many automated devices are developed and used in healthcare sectors to reduce treating complexities. The advanced automated systems are mostly based on the Internet of Things (IoT) network. IoT is a physical object comprising software, sensors, and other advanced technologies. The primary purpose of inventing an IoT network is to reduce communication complexity through the Internet. IoT can easily connect and exchange data over the Internet from one device to another. The IoT devices may be wired or wireless. Such IoT-based wired or wireless devices connect human-to-human or human-to-machine through the Internet, allowing them to communicate through the sensors.

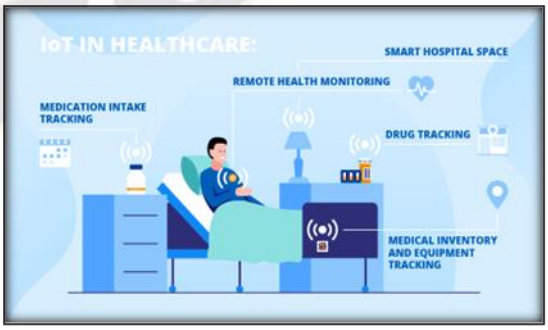

Figure-1. Internet of Things (IoT) devices in the healthcare industry

A sensor is a device that monitors the physical simulations and sends the signal to the server. Sensors in the IoT network create the interaction between humans and devices. Various protocols, like Zigbee, Wi-Fi, and Bluetooth,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

create interaction between the devices anywhere and at any time. IoT devices in hospitals are mainly used to observe and calculate blood pressure, heart rate, body temperature, and patient personal information maintenance. The IoT sensor is also used to monitor the medical equipment types like oxygen pumpsand nebulizers. The IoT-enabled system increases the possibilities of the remote monitoring system. The wearable IoT sensors are integrated into watches, garments, wristbands, and smartphones. IoT sensor analyzes the patient's health condition and stores it in the hospital database. Such data helps the physician to give treatment. The IoT sensor continuously monitors the health of the patient from any location. If it detects any changes in the patient's health, it immediately sends the signal to the physician for quicker treatment. Through the IoT device, a doctor can remotely guide the patient in taking first-aid steps to prevent them from becoming serious. The main advantage of implementing IoT device in the healthcare sector is cost reduction, advanced treatment methods, quick diagnosing, drug management, and continuous health monitoring. These advantages increase the efficiency of healthcare services.

Though HIoT increases the quality of the healthcare industries, the IoT-based healthcare system faces many challenges and issues. The major issues in HIoT are security and privacy issues, diagnosing issues, scalability, and trust. To overcome these issues machine learning algorithm is utilized. Machine learning is the branch of AI. ML algorithms can predict the output accurately without the help of predefined programs. Machine learning is divided into three types: supervised, unsupervised, and reinforcement. Each type performs various tasks like clustering, classification, and regression. And each type includes various algorithms like SVM, Decision Tree, Random Forest, linear regression, and NB. Through these algorithms, the machine learning model is combined with a set of IoT protocols to enhance the efficiency of data privacy and security in healthcare industries. In order to provide better security for healthcare IoT data, this paper has aimed to provide a better security solution, and thus it contributes:

- A healthcare IoT framework is created for IoT data generation.
- The Support Vector Machine algorithm is implemented for analyzing and classifying the HioT data.
- At each data transmission time over the healthcare framework, the RSA algorithm encrypts and decrypts the data.
- The experimental result is verified, and the performance is compared with the other algorithms.

The issues and challenges of the earlier research methods must be identified before planning or designing the proposed research work. So, a detailed literature review has been carried out.

II. LITERATURE SURVEY

K. Mandula et al. (2015) in this paper researcher discussed IoT and how IoT can be used to recognize smart home automation and utilize a micro-controller-based Arduino and Android mobile app. Two prototypes, namely home automation operating Bluetooth in an indoor environment and also home automation operating Ethernet in an outdoor environment, are used in this paper.M. Farooq et al. (2015) detail the IoT framework and its analysis of authorized technologies and sensor networks. Also, the authors explain the six-layer architecture of IoT and denote the related key challenges.A. Kapoor (2016) explains in this paper whether environmental or manufactured factor hinders plant growth by developing an approach with a combination of IoT and image processing. With the help of an IoT sensing network, the readings of the important environmental factors and the image of the leaf lattice are taken. A histogram analysis is done using MATLAB software to arrive at the final results.Alam F et al. (2016) have studied the applicability of various popular data mining algorithms, which also include deep learning artificial neural networks (DLNNs) that build a feed-forward multi-layer artificial neural network (ANN) for IoT data. Though the two networks, ANNs, and DLANNs, are computationally expensive, they give better results. Three IoT datasets show that C4.5 and C5.0 have better accuracy, memory efficiency, and high processing speed.

L. Banica et al. (2017) A new concept, namely Internet-of-things (IoT) in IT&C (Information Technology and Communications), is presented in this paper. A study to show the importance of applying IoT in higher education is conducted after introducing this concept briefly. The researchers identified many practical methods for integrating IoT features in academia, particularly in teaching and learning enhancements. Many IT&C companies have launched and implemented projects in the field of education, but a model for "Smart Universities" is unclear. The authors have proved that using IoT platforms with cloud computing was the best technical solution in education.

Thakar et al. (2017) have emphasized the importance of using IoT with multiple sensors in medical checkups. The data from the device helps the doctors analyze them and accordingly give the best service to the patients. It also helps to generate medical reports. The authors have highlighted the opportunities and challenges for the future usage of IoT in healthcare. The authors have also suggested that smart systems

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

should be designed to present sustainable medical intervention and manage time because health care is one of the most delightful and important fields. The smart system should also be simple, have low energy consumption, and have real-time feedback. It ensures avoiding unnecessary hospitalizations, reduce the total cost of health care, and give patients speedy care.S., Chenget al. (2017) have discussed the complexity of personalized service due to the increasing number of medical sensors. It results in a waste of resources and an increase in the response time. So, the authors have in this paper proposed a hierarchical fog-cloud computing CEP architecture. It can accelerate the personalized service response time and reduce resource wastage. In the first two steps, the authors have introduced the architecture, including the sensor, fog, and cloud layers, and proposed a series of optimization for the architecture. The authors have used a partitioning and clustering approach and a parallel processing policy to optimize fog and cloud computing. They have used an architecture named FogCepCare for implementing a prototype system. The result showed that FogCepCare architecture was better than traditional IoT-based healthcare.

Djenna and D. E. Saïdouni (2018, October) have given an overview of security issues in IoT-based healthcare applications. They have stated the issues that are varied from other domains. Some of the issues are in terms of methodologies, motivations, consequences, varying degrees of complexities of the environment, and the nature of deployed devices. They have also provided a new classification of cyber attacks that could affect the functioning of such infrastructures, in addition to discussing their threats and vulnerabilities.S.Islam et al. (2015) have stated that smart objects are the building blocks in developinga cyber-physical smart pervasive framework.

Moreover, the IoT has a variety of applications in various domains and has revolutionized modern health care with bright prospects. The researchers have surveyed the advancement in IoT-based healthcare technologies and reviewed the industrial trends in IoT-based healthcare solutions. They have also analyzed the security and privacy features, threat models, and attack taxonomies from the view of healthcare. Furthermore, they have proposed an intelligent collaborative security model to minimize security risk and address different types of IoT and healthcare policies and regulations worldwide. They have discussed the innovations that could be leveraged in a healthcare context. It should provide more avenues for future research on IoT-based healthcare.

Tyagi S et al. (2016- January) predicted that various fields such as domestic, smart homes, healthcare systems, goods monitoring, and logistics would see a technological revolution due to the application of IoT. They have listed the applications of IoT AND addressed some important parameters and features of each application. They have also explored the role of IoT in healthcare and examined the opportunities. Finally, they have proposed a cloud-based conceptual framework to benefit the healthcare industry and provide solutions for its implementation.J., Yang, et al. (2017) have initially briefed the challenges and issues in the usage of IoT, like shortage of cost-effective medical sensors, substandard IoT system architectures, high demand for interoperability, and so on. They have also stated that a new internet revolution is rapidly occurring, and new research in many fields and disciplines is becoming more popular. They have systematically reviewed advanced IoT-enabled PHS to solve the problems mentioned above. It helps to review key enabling technologies and successful case studies in healthcare and ultimately refer to future research trends and challenges.

S.Gopalan et al. (2021) have suggested considering the security challenges in the early design stages in any digital transformation in modern healthcare. Since healthcare data is more sensitive, any breach can damage patients' privacy. Moreover, the connected devices in IoT networks are open to Cyber attacks that can cause adverse consequences. In this paper, the researchers have thoroughly analyzed research papers between 2014 and 2019 to determine the use of AI to protect IoT networks. Researchers can also focus on this area In the future after thoroughly analyzing a related paper.F.Aktas et al. (2018) IoT-based biomedical applications are widely used in various systems such as healthcare, diagnosis, treatment, and monitoring. Enabling technologies are also important components of IoT concepts. The authors have built a new IoT-based healthcare framework for using hospitals using Riverbed Modeler Software. Also, using this framework and forming a time-saving simulation environment, some case studies in hospital information systems can be realized.

J.Hou (2015) stated that the IoT, or the network consisting of interconnected objects, as it is otherwise called, is the result of the advancement in information communication technologies. Research and development of security for IoT-based applications have seen great advancement. The authors have proposed an architecture based on sensor tags for IoT-based healthcare systems. Also, a secure authentication scheme and a robust protocol for IoT-based healthcare systems have been proposed. The robustness of the proposed schemes is proven under adverse conditions.

The healthcareIoT has data privacy, which is the major challenge in IoT when all the IoT devices transmit their real-time data. The attacker, like a "man-in-the-middle," hacks the data when the connection is not secured. Since the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

healthcareIoT is huge in volume, handling the data accuracy may create issues. The cost of the data analytical model and securing the data is too high. Also, the cybersecurity risks, patient isolation, and frustration with poor implementation are some of the limitations present in the earlier research works. This paper provides an SVM model for data classification where it can separate personal and sensitive data to secure it to overcome these limitations,. The RSA algorithm is used for cryptographic operations over the personal/sensitive data generated from the healthcare IoT network.

III. PROBLEM STATEMENT

Health Insurance Portability and Accountability Act (HIPAA) rules place a high priority on medical database safety. According to the HIPAA protection act, Regulated companies must evaluate data protection measures through threat analysis and implement a threat management theory as a remedy for any risks found. Confidential patient information may be accessed by the intruder and taken. Additionally, the intruder may change patient records mistakenly or on purpose, which could negatively impact the wellness of patients. Therefore, security becomes paramount when it comes to medical data. In order to address this problem, it is assumed that **L** numbers of Health Care Data Managers (***HCDMgr***) are allotted to enter the health records of every individual patient.

$$\boldsymbol{HCDMgr} = \{\boldsymbol{HCDMgr_1}, \boldsymbol{HCDMgr_2}, \dots, \boldsymbol{HCDMgr_i}, \dots, \boldsymbol{HCDMgr_L}\} \quad \forall \boldsymbol{i} = \boldsymbol{1\ to\ L}$$

The data that has to be entered in the cloud database can be collected from N number of hospitals and are fed into the cloud database by the $\boldsymbol{HCDMgr}$.

$$\boldsymbol{D} = \{\{\boldsymbol{D_1}\}, \{\boldsymbol{D_2}\}, \dots, \{\boldsymbol{D_i}\}, \dots, \{\boldsymbol{D_N}\}\} \quad \forall \boldsymbol{i = 1\ to\ N}$$

The term $\boldsymbol{D_i}$ denotes the collection of M number of patient data.

$$\boldsymbol{P} = \{\boldsymbol{P_1}, \boldsymbol{P_2}, \dots, \boldsymbol{P_i}, \dots, \boldsymbol{P_M}\} \quad \forall \boldsymbol{i = 1\ to\ M}$$

The data can be in the form of text, image, audio, video, etc.,

$$\boldsymbol{Database} = \{\boldsymbol{text}, \boldsymbol{image}, \boldsymbol{audio}, \boldsymbol{video}\}$$

The data mentioned above are stored in the cloud database using encryption. Also, $\boldsymbol{HCDMgr}$ are provided with a unique security key thathelps encrypt the data into the database.

Encryption

An asymmetrical encrypting method that is frequently utilized in various goods and businesses is Rivest-Shamir-Adleman (RSA).Asymmetrical encrypting encrypts and decrypts the information using a couple of connected keys statistically. The creation of a key couple results in the creation of a hidden and open key. The hidden key remains confidential, accessible solely to the key couple's inventor.Using RSA, the information can be encrypted using either the hidden or open key and decrypted using another key.This is among the factors that make RSA the widely utilized asymmetrical encryption technique. Encrypting using the hidden or open key offers RSA operators a wide range of benefits. If the material is encrypted using the open key, it must be decrypted using the hidden key. The technological aspects of RSA are based on the assumption that while combining two adequately huge numbers simultaneously is simple, it is challenging to factorize the result into the underlying prime integers. Two digits are a composite of two enormous prime figures used to construct the open and hidden keys. Both derive their values from identical pairs of prime integers. The typical size of an RSA key is 1024 or 2048 bits, proving it very challenging to factorize it, although 1024-bit keys are rumored to be likely to crack fast.

The stated problem statement is represented in Figure-1. There is an $\boldsymbol{N}$ number of users who wants to access data and fetch the data. This fetching process would be carried out by verifying the user information by the mechanism of user authentication and authorization. Followed by that, the user would be accessed with permission to fetch data from the cloud database that contains the healthcare data of many patients. The user data fetching also includes a data decryption model that is stacked to provide improved security.The N number of users can be represented as $\boldsymbol{U}$.

$$\boldsymbol{User}, \boldsymbol{U} = \{\boldsymbol{U_1}, \boldsymbol{U_2}, \dots, \boldsymbol{U_i}, \dots, \boldsymbol{U_N}\} \quad \forall\ \boldsymbol{i = 1\ to\ N}$$

Data Authentication And Authorization

Numerous methods can do data authentication and authorizationto improve the security of IoT. There are several reasons for IoT getting trapped in the hands of breaches. Initially, previously unconnected objects are linked to the Web, a hostile landscape packed with prospective attackers.Moreover, since computers lack suitable accessibility restriction methods, the interconnected devices were not durable sufficiently to be left out in the badlands.

The method of deciding if a system or individual has entry to services, such as the ability to receive or create information, run programs, or regulate, is known as accessibility management, sometimes known as authorization. Rejecting or withdrawing access is another authorization aspect, particularly regarding anything or anyone dangerous.Authorization is a requirement for authenticating, a procedure for recognizing an individual. Absent adequate authentication, authorization is frequently not even feasible.The foundation of authentication is trust. For instance, in order to examine somebody's ID, one should initially have

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

faith in the organization that issued it, such as a hospital that provided it.Computers that are connected to the network also possess a very similar ideology. The mechanism mainly focused on implementing confidentiality among the browsers, which act as a client, and the accessing database website, which acts as a server. Numerous websites utilize HTTPS, which is a safe design of HTTP. It operates with SSL or TLS protocols employed to offer channel safety.

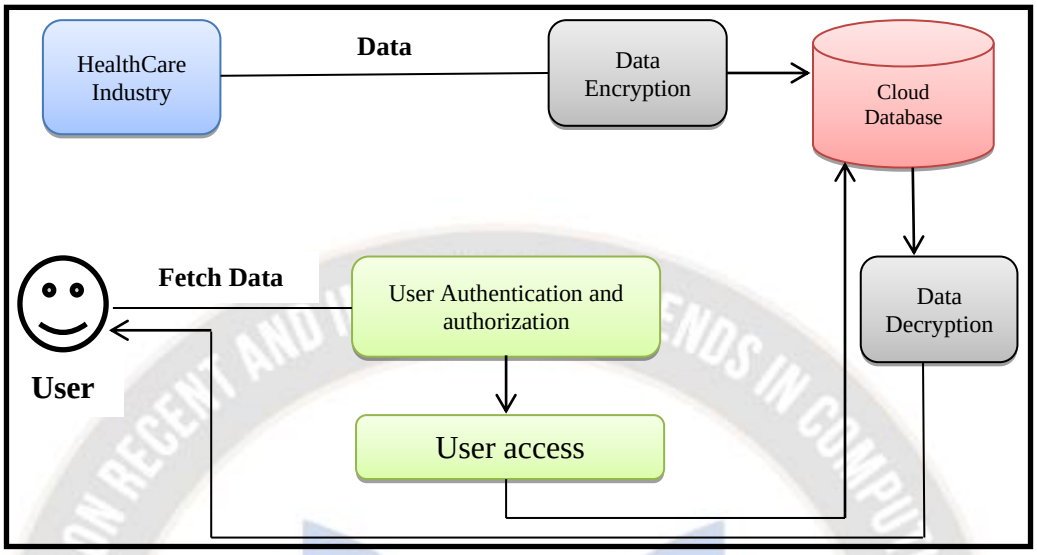

Figure-1. Representation Of The Proposed Problem Statement

These protocols utilize open-key cryptographic technology to develop a channel; hence, the server's open-key authentication is essential. A (virtual) credential, a symbol for authenticating, contains the open key of the server.A credential administrator (CA)is responsible for issuing and electronically signing certificates. The browser has faith in the CA because it has granted a credential for the healthcare database website. The internet server shows the browser its credentials whenever it links.With the CA's accreditation, the browser validates the user's credentials.The browser believes the healthcare website if the validation is successful.A collection of responsibilities and guidelines for distributing and administering those credentials is known as an open-key architecture (OKA).Symbols can be used in various techniques to authenticate users in computer networks. The more popular method for authenticating human users is with a passcode.

Cryptography is a valuable technique for ensuring protection in machine-to-machine connections. People frequently utilize two-factor authentication to tighten protection by utilizing everything humans possess (like cell phones) and who humans are (like biometrics) in combination with what humans know (passcodes).Cryptographic keys are frequently employed as symbols for authentication and authorization in this crypto network.

User Access Permission

The user can enter the patient's details, such as user id, passcodes, and metadata. The machine learning algorithms are used by training the network with the exact user details and login credentials. The machine learning algorithm verifies the login credentials and user details entered by the user while fetching data from the health care database with the trained database. The machine learning algorithm in this proposed architecture is a multiclass Support Vector Machine (Multiclass SVM). Once the details are verified and validated, the decryption takes place.

Data decryption

The user must enter the proper credentials to access the data—the security key provided to the individual $\boldsymbol{HCDMgr}$is transmitted to the user who correctly entered the credentials. With the help of the specific security key, the user can access the data, and thus, data decryption takes place.

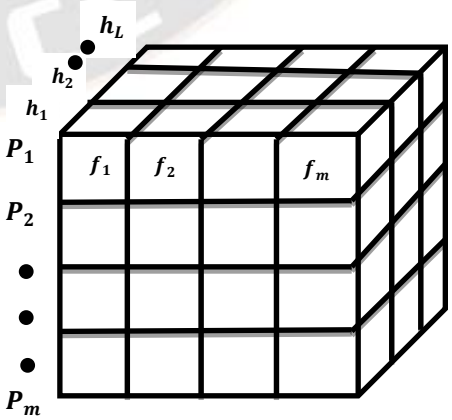

Figure-2. Representation of data in Matrix

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

Multiclass Support Vector Machine

SVM is a supervised machine learning technique that supports problem statements for regression and classification. Based on the chosen kernel value, SVM performs sophisticated data operations. It looks for a hyper-plane, or ideal border, among distinct classes. Depending upon those transitions, SVM seeks to maximize the divergence borders among the data units. SVM seeks to locate a line that optimizes the distance among a two-class data set containing 2-dimensional space objects in its most basic configuration, where it is a linear divergence. SVM aims to identify a hyper-plane in an n-dimensional domain that optimizes the distance between the data units and their corresponding classes. Support vectors are the data elements nearest to the hyper-plane and have the smallest spacing. Figure-3 depicts the support vectors.

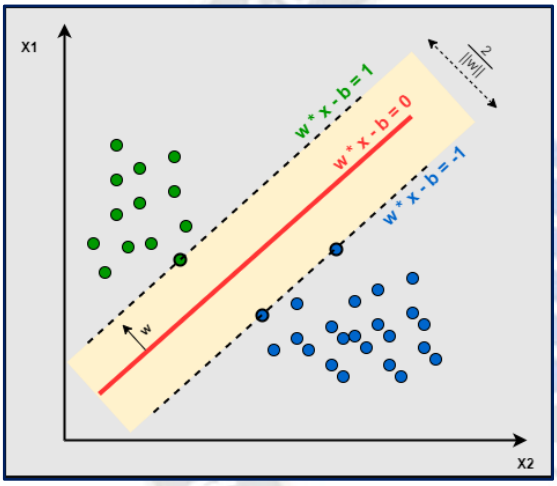

Figure-3. Support Vectors

SVM does not support multiclass classification in its most basic form. Following the multiclass classification issue's breakdown into simpler subtasks, and binary classifier issues, the identical method is applied. The one vs. All (OVA) technique is typical for multi-classifying problem statements utilizing SVM.

One vs. All (OVA) technique

In this approach, one may possess ***N*** class issue, and the model may need to learn N SVMs:

SVM $\mathbf{N_1}$ learns "class_Outcome=**1**" vs "class_Outcome≠**1**"

SVM $\mathbf{N_2}$ learns "class_Outcome=**2**" vs "class_Outcome≠**2**"

:

SVM $\mathbf{N_N}$ learns "class_Outcome=**N**" vs "class_Outcome≠**N**"

To estimate the outcome of the novel input, one may estimate with every unit of the constructed SVMs and consequently obtains the unit that keeps the estimation to the highest distance into the positive area. One should also notice the shortcomings of training the SVM-N network. There may be an issue of unbalancing arise. When there are 10 classes, ranging from 0 to 9, and you get 1000 data per class, each SVM with two classes would contain one class with 9000 data and another with just 1000 data units, making our situation unbalanced. The 3-Sigma rule or SMOTE subsampling technique can address this issue. Consider one possesses multiclass issues that have K categories, then for the N^{th} classifier:

- Positive Samples: all the points in class $N(\{\boldsymbol{X_i}: \boldsymbol{N} \in \boldsymbol{Y_j}\})$.
- Negative Samples: all the points in class $N(\{\boldsymbol{X_i}: \boldsymbol{N} \notin \boldsymbol{Y_j}\})$.
- $\mathbf{f_N(X)}$**:** the value of the decision for the N^{th} classifier.

If the value of $\mathbf{f_N}$ is high, then there is a greater probability for X to be in the class N

- Estimation: $\boldsymbol{f(x) = argmax_t f_N(X)}$

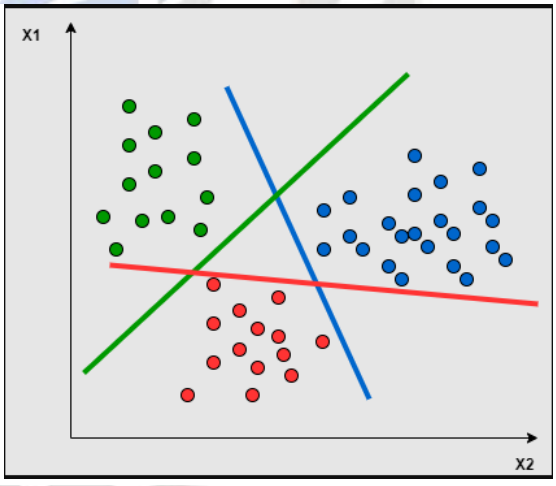

Figure-4. One vs. All Technique

One may attempt to correlate the hyper-plane to diverge the classes in this technique. The divergence accepts all the data and eventually separates it into groups. In those groups, there is one group for the one class data unit and the group for all the other data units. For illustration, in Figure-4, the Green line attempts to simultaneously increase the separation among green data units and other points.

Experimental Results and Discussion

The proposed SVM-RSA algorithm is implemented in Python and experimented with sample data. The execution is on Intel Pentium, a 7^{th} generation core-i7 processor with

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

2.64 GHz speed, 1TB HDD, and 8GB RAM. The obtained results are compared with other classification algorithms like Ada Boost Algorithm (ADB), Naïve Bayes algorithm, and Support Vector Machine with the proposed multiclass SVM.

Detecting a classification model that provides better classification without imbalance is very much difficult because of its varied accuracy with the nature of the data. The dataset considered is divided and plotted in the graph. The x-axis represents various classes, and the y-axis represents the number of samples in various classes. The dataset consists of uneven data that must be classified and distributed uniformly. The traditional classification models compare each data with every class and classify them, which consumes more resources and also failsin harder situations. Based on the class-wise classification, the size of the classes are 13234, 47394, 94857, 39485, and 31928. The imbalance ratio of the dataset is 4.35. This comparison aims to show that the proposed algorithm performs well against other classification algorithms. It also tries to reduce the imbalance in the dataset as much as possible. Various methods are proposed from time to time to reduce the imbalance of the dataset. But, only a few used class-based classification to classify the data. The class-based classification can be effectively done through the multiclass SVM algorithm. It helps in making an efficient healthcare system through IoT technologies. Four classification algorithms mentioned before are compared here, and the performance metrics are evaluated. It is compared based on suitability, correctness, and efficiency. Likewise, ten performance measures are considered to compare the algorithms. The figure-5 shows the overall participation of the classification algorithms with the existing method. The performance evaluation consists of two parts. The first part compares the precision, recall, and F1 score of all the algorithmswith the proposed algorithm. In the algorithms considered here, Ada Boost Classifier provides the lowest performance numbers in Table-1. The other algorithms and the proposed ones provide better performance numbers in reducing the data imbalance. The proposed algorithm outperforms other algorithms in the data imbalance reduction and better classification of the data through multiclass classification. It can be seen in Table-1.

Table-1. Performance Comparison

Classification algorithm	**Precision**	**Recall**	**F1-Score**	**Accuracy**
Ada Boost classifier	0.56	0.6	0.54	60.45
Multi-Layer Perceptron	0.92	0.94	0.968	95.71
Naïve Bayes	0.88	0.85	0.87	80.87
Support Vector Machine	0.94	0.95	0.95	97.76
Multiclass SVM	0.99	0.98	0.99	99.52

In the second part, the overall performance of the proposed is compared with other existing algorithms in the literature. It can be seen from the table-2 that the proposed algorithm outperforms other algorithms considered in the table from the existing methods in the literature. The dataset is classified into various classes, and each data is compared and classified into the present classes. There is a fixed number of classes; the entries in the datasets are classified within the present classes. The proposed algorithm achieves an accuracy of 99.72 percent.

Table-2. Comparison In Terms of Accuracy

Model used	**Accuracy (%)**
Cost-sensitive Boosting[41]	90.52
Cost-sensitive SVM [43]	95.01
Fuzzy-based SVM [44]	97.19
Improved SVM [46]	97.51
Improved SVM [49]	96.90
Proposed Model	99.52

The data obtained from the healthcare dataset are classified based on their nature. The quality of the healthcare data is very poor, leading to an imbalance in the data. It is because of the technical glitches in IoT technology. So, the dataset obtained directly from the IoT networks needs to be screened to identify vague and unrelated data in the overall dataset. It is called the pre-processing of the dataset. During this process, the unrelated or vague data obtained due to technical glitches can be removed, and the data quality is improved. It is done through a famous method called missing values or outliers. This method helps in finding the problems in the dataset.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

Table-3. Cross Validation Comparison

Data Samples Classified	Classification Algorithms				
	Ada Booster	Multi-layer Preceptron	Naïve Bayes	Support Vector Machine	Proposed Algorithm
A1	67.97	87.37	84.1	95.78	99.64
A2	54.1	75.73	83.84	95.43	99.47
A3	69.87	76.4	82.01	96.07	99.6
A4	67.04	82.33	85.74	96.01	99.61
A5	85.71	91.17	83.64	95.89	99.45
A6	68.36	84.34	86.92	95.21	99.48
A7	69.45	91.17	81.83	94.18	99.5
A8	68.57	91.88	82.34	96.73	99.85
A9	69.01	85.81	85.94	96.57	99.62
A10	74.82	92.38	86.01	98.41	99.74
A11	61.61	87	84.07	96.28	99.54
A12	86.55	91.19	83.41	97.35	99.65
A13	68.68	88.11	79.47	97.35	99.66
A14	98.42	66.34	83.7	96.04	99.61
A15	64.77	86.46	84.06	94.51	99.08
A16	67.75	86.3	82.85	97.37	99.23
A17	64.72	78.57	82.27	96.75	99.45
A18	73.82	92.75	82.42	97.34	99.75
A19	69.01	90.74	85.46	98.19	99.24
A20	71.6	88.72	81.41	95.29	99.78
A21	70.12	86.34	85.56	96.76	99.55
A22	76.3	74.84	83.46	96.36	99.71
A23	81.99	91.77	82.93	95.56	99.56
A24	74.49	91.58	84.92	95.68	99.46
A25	70.61	78.09	84.02	97.29	99.58
A26	92.92	83.88	80.69	95.55	99.25
A27	67.48	79.72	82.79	97.21	99.53
A28	66.48	84.96	84.65	95.78	99.56
A29	73.17	92.7	84.21	97.56	99.56
A30	65.92	87.68	85.07	95.58	99.18
A31	65	92.03	81.25	95.3	99.38
A32	70.57	85.78	81.21	92.75	99.33
A33	89.56	93.43	83.76	97.13	99.43
A34	73.51	91.69	80.98	96.36	99.4
A35	64.47	91.72	84.13	95.75	99.54
A36	83.59	86.21	86.06	97.54	99.41
A37	79.75	71.78	84.73	97.24	99.37
Total Accuracy	72.64216	85.91784	83.56514	96.27432	99.50676

Cross-validation

It is the process of evaluating the performance of the proposed algorithm; the dataset is classified into n number of datasets and is subjected to n-fold cross-validation. The n classified samples have an equal number of samples in each, which is used to evaluate the proposed algorithm. The n classified samples are divided in the ratio of 4:1 for the training and testing sets. The training sample trains the model, and the testing samples test the proposed model. The performance obtained from all the algorithms considered in this paper is shown in detail in figure-7.

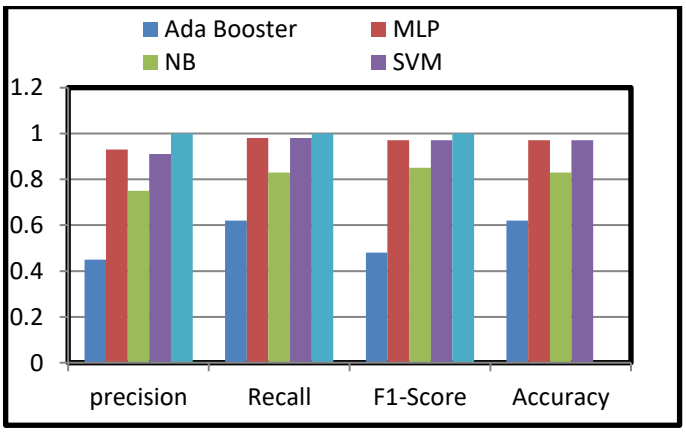

Figure-5. Performance Comparison

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

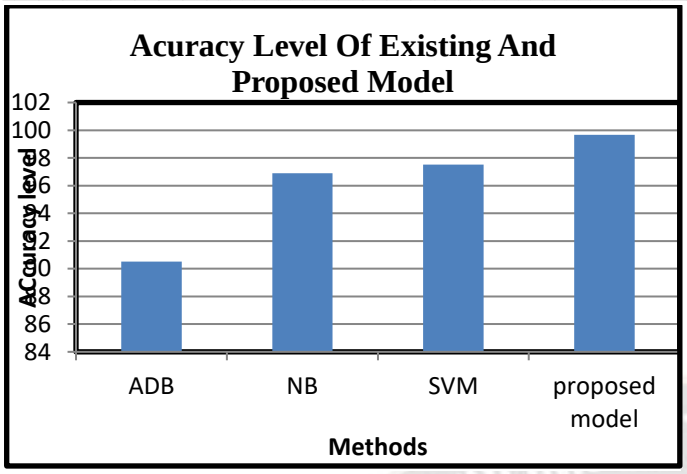

Figure-6. Accuracy Comparison

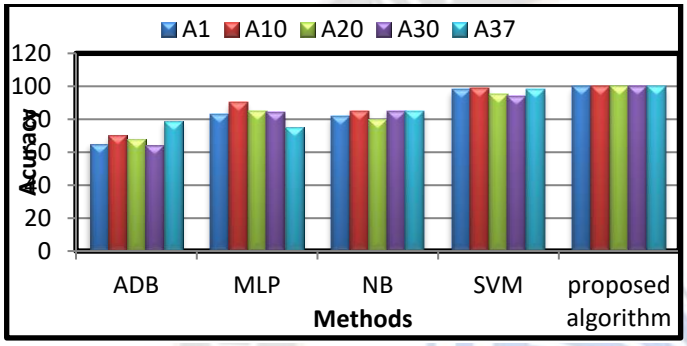

Figure-7. Cross Validation Accuracy

The figure-7 shows the classification algorithms' accuracy and the variations with the change in the data samples. This helps evaluate the algorithm's performance at varied levels of imbalance. All the algorithms differ in the accuracy level with different samples, while the proposed provides constant and higher accuracy over every sample. Figure 9 shows the performance of the algorithms in various dataset samples. It can be seen that the proposed algorithm is consistent in all the samples, while the other algorithms fluctuate in the actual performance.

IV. CONCLUSION

This paper aims to provide high-level security for healthcare IoT data. A healthcare network is assumed with ***N*** number of IoT devices connected. Each IoT device is attached or linked with any one of the patientsat various time intervals. All the devices generate a high amount of data,which secures privacy and sensitivity. This paper uses two different concepts called clustering-classifying and encryption-decryption. All the data are initially fed into a support vector machine algorithm for clustering and classification. Then RSA algorithm is used for encrypting and decrypting the privacy and sensitive data of the patients. From the experiment, this proposed SVM-RSA algorithm provides a good accuracy (99.52%) compared with the other algorithms. This paper reduced the overall computational time by focusing on only privacy and sensitive data.

Future Work

In future work, the real-time data is fed into SVM-RSA, and the performance needs to be verified.

Reference

[1] Mandula, K., Parupalli, R., Murty, C. A., Magesh, E., & Lunagariya, R. (2015, December). Mobile-based home automation using the Internet of Things (IoT). In 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 340-343). IEEE.

[2] Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review ofthe Internet of Things (IoT). International journal of computer applications, 113(1), 1-7.

[3] Kapoor, A., Bhat, S. I., Shidnal, S., & Mehra, A. (2016, October). Implementation of IoT (Internet of Things) and Image processing in smart agriculture. In 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 21-26). IEEE.

[4] Alam, F., Mehmood, R., Katib, I., & Albeshri, A. (2016). Analysis of eight data mining algorithms for smarter Internet of Things (IoT). Procedia Computer Science, 98, 437-442.

[5] Banica, L., Burtescu, E., & Enescu, F. (2017). The impact of internet-of-things in higher education. Scientific Bulletin-Economic Sciences, 16(1), 53-59.

[6] Thakar, A. T., & Pandya, S. (2017, July). Survey of IoT enables healthcare devices. In 2017 International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1087-1090). IEEE.

[7] He, S., Cheng, B., Wang, H., Huang, Y., & Chen, J. (2017). Proactive personalized services through fog-cloud computing in large-scale IoT-based healthcare applications. China Communications, 14(11), 1-16.

[8] Sunil Patil, Rakesh Saxena, Yogesh Pahariya. (2023). Performance Comparison of SRM, PMSM & BLDC Motor Drives via Experimentation in Laboratory for EV Application. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 405 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2736

[9] Djenna, A., & Saïdouni, D. E. (2018, October). Cyber attacks classification in IoT-basedhealthcare infrastructure. In 2018 2nd Cyber Security in Networking Conference (CSNet) (pp. 1-4). IEEE.

[10] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of things for health care: a comprehensive survey. IEEE Access, 3, 678-708.

[11] Tyagi, S., Agarwal, A., & Maheshwari, P. (2016, January). A conceptual framework for IoT-based healthcare system using cloud computing. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 503-507). IEEE.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7795
***Article Received**: 22 May 2023 **Revised:** 20 July 2023 **Accepted:** 10 August 2023*

[12] Qi, J., Yang, P., Min, G., Amft, O., Dong, F., & Xu, L. (2017). Advanced Internet of things for personalized healthcare systems: A survey. Pervasive and Mobile Computing, 41, 132-149.

[13] Christopher Davies, Matthew Martinez, Catalina Fernández, Ana Flores, Anders Pedersen. Applying Recommender Systems in Educational Platforms. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/171

[14] Gopalan, S. S., Raza, A., & Almobaideen, W. (2021, March). IoT security in healthcare using AI: A survey. In 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1-6). IEEE.

[15] Aktas, F., Ceken, C., & Erdemli, Y. E. (2018). IoT-based healthcare framework for biomedical applications. Journal of Medical and Biological Engineering, 38(6), 966-979.

[16] Hou, J. L., & Yeh, K. H. (2015). Novel authentication schemes for IoT-based healthcare systems. International Journal of Distributed Sensor Networks, 11(11), 183659.