Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 30 No. 4 (2023)

Revolutionizing the Medical Record Department with a Blockchain-Enhanced Nonlinear Approach to Medical Record Management (MRM) Systems

Mona Mulchandani[1] Priti Samrit[2], Palak Tahlyani[3], Srushti Wakode[4], Iqra Ansari[5], Muskan Sheikh[6]

Department of Computer Science and Engineering, Jhulelal Institute Of Technology, Nagpur, Maharashtra, India
hod.cse@jitnagpur.edu.in[1], pritisam12@gmail.com[2], palaktahlyani@gmail.com[3], wakodepratiksha243@gmail.com[4], iqrazangggsari1999@gmail.com[5], jitcse.muskansheikh@gmail.com[6]

Article History:

Received: *15-08-2023*

Revised: *18-09-2023*

Accepted*: 10-10-2023*

Abstract:

This work presents a thorough design and construction overview in order to meet the impending issues associated with conducting a groundbreaking project. The centerpiece is a cutting-edge, specially designed for government dentistry institutions, Blockchain-Enhanced Nonlinear Approach to Medical Record Management Systems. The system's goal is to keep patient data safely while offering a user-friendly interface, reliable backup systems, and security. In the first stage, a blockchain-based medical record system will be put into place, and medical staff members will be asked for vital information to be authenticated. The ability to save and manage patient data, including crucial information like patient classifications, is subsequently provided to these verified individuals. The system determines a patient's eligibility to pay medical care costs by intelligently classifying them into groups. For example, BPL holders, elderly residents, and convicts are not required to pay for medical care. This paradigm places a high priority on security, and the article presents the idea of cryptography inside the blockchain. A secret common key is used to assist the encryption and decryption operations that are applied to data. Sensitive medical information is protected by this cryptographic technique, which guarantees the secrecy of discussions between two entities. The data may be retrieved by using this private key, which guarantees the privacy and availability of patient records that are saved.

Keywords: Medical Global E-commerce, Smart Access, Clinical Information, Health Systems, Network Security, Reporting Capabilities, Non-linear Approach.

I. Introduction

This study presents a novel Blockchain-Enhanced Nonlinear Approach to transform Medical Record Management Systems in response to the emerging issues encountered by government dental institutions in handling increasing patient data. Conventional approaches find it difficult to handle the increasing volume of data, which calls for a nonlinear paradigm change in favor of blockchain technology. The web application incorporates a nonlinear security structure and consists of OPD receptionist, cashier, and admin modules. Blockchain cryptography-based encryption and decryption methods provide a high-level of security for private patient data. This nonlinear encryption method offers a smooth way to retrieve data while guaranteeing data integrity and making it impervious to tampering.

Unlike traditional fee collecting techniques, the cashier module determines charges on its own by using patient classifications. This adds intelligence to the system, minimizes mistakes, and guarantees transparent financial transactions in addition to streamlining the fee collecting process. As the highest authority, the admin module performs nonlinear verification and retrieval to guarantee the correctness and completeness of patient data.

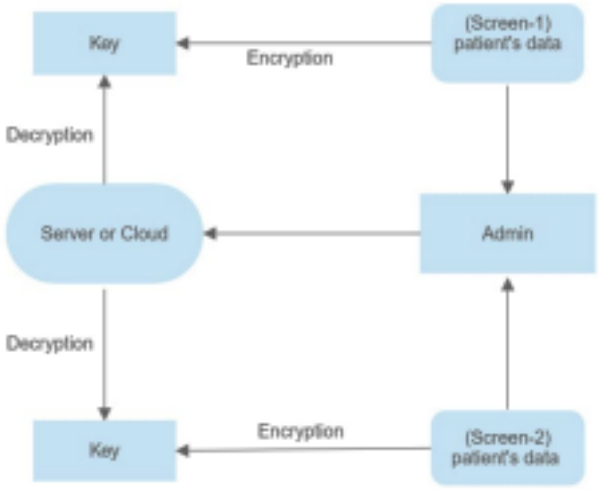

Figure 1. General MRD System

The blockchain-based solution addresses the problems associated with math mistakes and computation errors, posing a nonlinear challenge to traditional data management techniques. The use of asymmetric cryptography techniques marks a significant advancement in data interchange security. Public key transmission, encryption, and the decryption procedures that follow provide a stable and nonlinearly transparent data flow.

In addition to being very secure for data, this technology brings nonlinear improvements in healthcare. A significant advancement in patient tracking that gives doctors the ability to make timely and well-informed decisions is real-time progress tracking. By facilitating prompt access to precise patient information, the system enhances the overall quality of healthcare services by nonlinearly reducing errors. By implementing blockchain technology, government dental hospitals are moving toward safe, effective, and cutting-edge medical record administration. This is an example of a nonlinear progression.

II. Literature survey

In this work, we propose that health systems should adopt intelligent access to need-based clinical data, offering a practical and remotely accessible option. The seamless progression of technology has streamlined consumer interaction with international e-commerce within the medical domain. Our main goal is to ensure safe communication between servers and clients, with an emphasis on network security [1][2]. These kinds of systems are required since certain healthcare providers' informational systems lack sufficient reporting capabilities, which makes it difficult for them to comply with business demands and accreditation criteria. The development of online platforms is prioritised as a result of providers turning to manual report production for clinical and administrative healthcare informatics difficulties [3-7].

Our research focuses mostly on the construction of hospital websites, but it also includes government dentistry and medical institution websites. We divide up patient data in accordance with hospital policies and put measures in place to stop theft or illegal changes. Our suggestion encrypts patient data using algorithms at the server end before transfer to prevent data theft and guarantee patient privacy. The privacy of the patient's information is also protected by this encryption [8]. Using several cryptographic ideas across our system—including the safeguarding of login credentials—we use 3DES and LSB to improve storage sharing, management, and strengthened security protocols against breaches of medical data, which are often the result of criminal attacks. Message encryption with symmetric keys adds even more protection to the system [9].

Our cashier module makes sure that the fee collection procedure is transparent and error-free by automating the collection of patient fees based on the patient's classification and standard rates invoiced to third parties [10]. With more power inside the hospital, the admin module makes effective data management easier by obtaining patient data as needed. Blockchain technology shows up as a key component that improves data management while also supporting patient data protection [11]. One significant benefit is the ability to follow a patient's development in real-time, providing medical personnel with up-to-date information. Reducing mistakes and improving diagnosis accuracy are made possible by having access to complete and accurate patient records. it is critical to use cryptographic approaches to protect sensitive patient data confidentiality and privacy. Our integrated approaches ensure a safe, encrypted environment that is only available to authorised users [12]. Incorporating these technologies is essential to improving patient care and fulfilling the demands of the healthcare sector. It is expected that healthcare practitioners will use these systems more frequently as technology advances in order to improve patient care and data management.

Table 1. Related Research

Application Area	**Approach**	**Methodology**	**Findings/Contributions**
Smart access to clinical information in health systems[3]	Network security for server-client communication	Implementation of online systems to meet business and accreditation needs	Development of a hospital website, encryption of patient data using algorithms for security
Enhancing security measures for medical data [4]	Combination of 3DES and LSB	Dependable and safe storage, sharing, and management	Improved security through symmetric key encryption, avoidance of data breaches
Hospital data administration and fee collection [5]	Automatic fee collection and efficient data administration	Blockchain technology for real-time tracking of patient progress	Improved fee collection process, efficient data administration, real-time patient progress tracking
Cryptography techniques for patient data security [6]	Mix of methods for secure, encrypted, and restricted data access	Ensuring security and privacy of sensitive patient data	Crucial role of cryptography in healthcare data management, anticipation of increased adoption of such systems with advancing technology

III. Proposed Methodology

Proposed system concern with map out design and assured security which is notably focuses on bifurgate the patient's data on the basis their category such as BPL holder , prisoner's,senior citizens,sc and so on.While building the application, we divided the models according to the use it is as follows receptionist, cashier, admin receptionist module Receptionist module is a module that will be display on first screen of project to gain the access of these module user must enter the appropriate secrete information.In this the user has put some required data about patients like name,uid,phone number,gender etc and according to it economic category is collect.the filled patient data are encrypted encoded with generating public key and the data is decoded in another end.and all the total bifurgated data average are directly store in the end of screen which the patient's information put. Cashier module it is second module in application which is inspired by first module the data of patient is same as first receptionist module but the bit change is it put the particular disease of the patient along with his fee the fees are mentioned automatically by fullfilled the potential corruption eventually about data average is converge at the last of screen and literally it pass on third module which is admin.

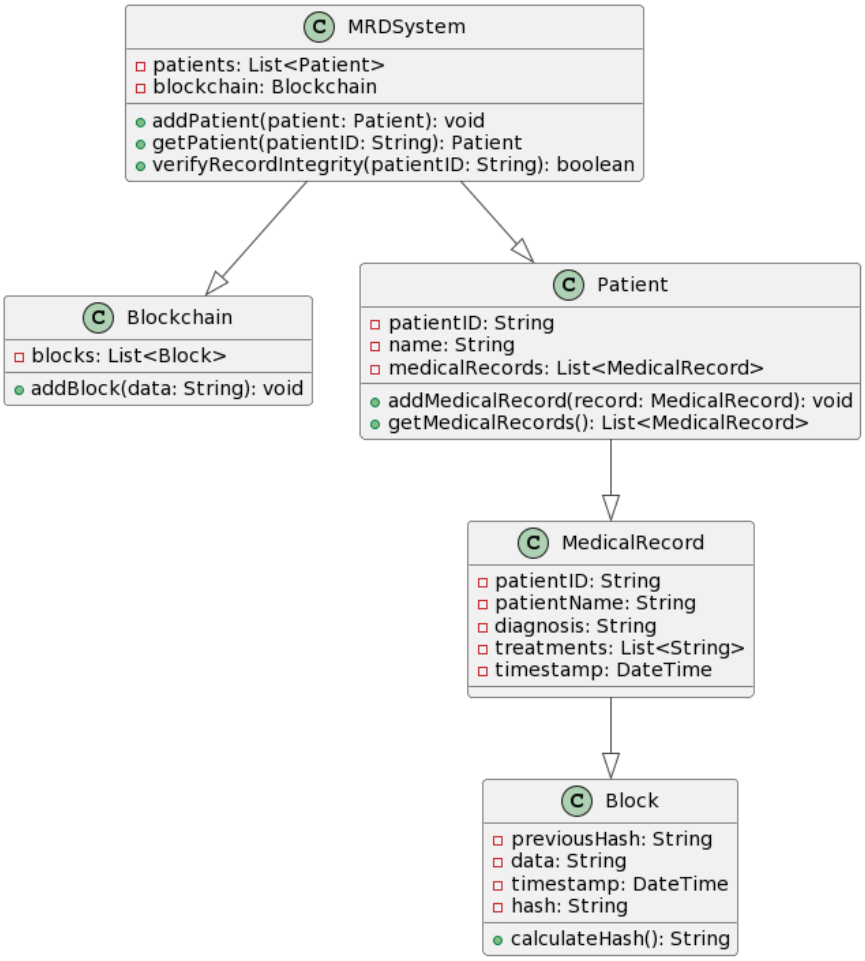

Figure 2. Proposed MRD System

The secure socket link (SSL) query pass encryption technique is base 64, sha256, len-40, and crc32.the Security Socket Layer, or SSL The safe hash algorithm (sha1), which encrypts data using a

cryptographic hash function, is the first method used in applications to keep data secure.It takes input data and transforms it into a 160-bit (20-byte) digest compressed form. The security socket layer is a method of creating a connection between a client and a server. In this instance, the client is a browser, and all algorithms send data end-to-end without being vulnerable to a middleman attack. The recommended approach uses encryption and security techniques together with a focus on application design. Three modules comprise the user interface: admin, cashier, and receptionist. Every module carries out a distinct set of duties. The user can enter the patient's economic category into the receptionist module, which is used to segment the patient's data. The data is subsequently encrypted using a public key and decrypted on the other end. On the other hand, the cashier module is in charge of recording the patient's particular condition and the related expense. There is no possibility of corruption because the expenses are generated automatically based on the illness. The procedure is finished by the admin module, which is also in charge of data storage security and system management. The SSL (Secure Socket Layer), base 64, SHA256, len-40, and CRC32 encryption and security techniques are used. SSL establishes a secure connection between the client and server, in this instance the browser. Using a cryptographic hash function, the data is encrypted using the SHA256 approach, resulting in a 160-bit digest. The CRC32 and Len-40 techniques can also be used to secure and encrypt data. All things considered, the suggested solution makes sure that patient data is protected against loss or unauthorised access and considers security concerns pertaining to medical data. To guarantee efficient processing of patient data, it also provides an easy-to-use user interface for the admin, cashier, and receptionist modules. A graph that compares the rate of factor utilised in these systems to comparable reference projects is available.

The logical presentation of this graph centres on the analysis of the data indicating the number of patients and the stage at which they are suffering tooth discomfort. We are able to predict that 10% of patients at dental clinical hospitals would experience significant issues with costly cement fillings based on the data analysis. The second stage is silver-coated, penny-costing cap filling, which is frequently performed on thirty percent of patients at dental facilities. Twenty percent of people get their teeth cleaned or have breathalysers fitted because it is less expensive than cement or cap fillings. The cleaning of teeth, which is the least expensive parameter and is utilised by around 40% of patients when they have dental-related problems, will be the last one we identify for this block graph. Most folks wanted this corrected as the first thing to happen. By comparing the patient data, an overview of this representation is created. Here, the visual aid determines the amount of data storage capacity and the time required for deployment. It also compares sites that have developed similar applications to ours, whose use cases are similar. After differentiating the system, the data storage limit is unlimited and depends on the host and type of application we use to store the data. If we choose to store data in the cloud, the cloud server we use will determine the amount of data we can store there. If we choose to save data on a personal server, there are maintenance restrictions. The graph above illustrates the ratio of how system updates occur on a daily basis, improving each system's ability to store an infinite amount of data through the usage of the SHA256 algorithm, which encrypts data while maintaining storage security. As SHA algorithm used to help the storage capacity so as the number of patients increase then it's will store in backend hence the scalibility rate is increased .

IV. Proposed Framework

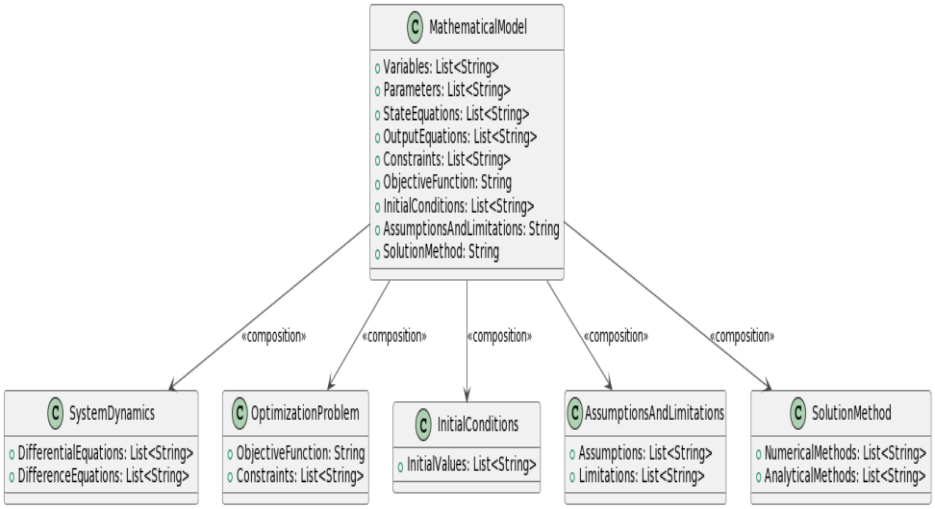

Figure 3. Proposed Framework

1. Variables:

- Let ($x_1, x_2, \ldots, x_n$) represent the state variables of the system.

- Let ($u_1, u_2, \ldots, u_m$) represent the control inputs or external influences.

2. Parameters:

- ($p_1, p_2, \ldots, p_k$) represent parameters affecting the system behavior.

3. State Equations:

- Describe the dynamics of the system using differential equations or difference equations.

$$(\frac{dx}{dt} = f(x, u, p)) \text{ or } (x_{k+1} = g(x_k, u_k, p)).$$

4. Output Equations:

- Express the system throughput with in terms of the state variables.

$$(y = h(x, u, p)).$$

5. Constraints:

- Include any constraints on the variables or inputs.

$$(x_i \geq 0) \text{ or } (u_j \leq 1).$$

6. Objective Function (if applicable):

- Define the objective function to be minimized or maximized.

$$(J = c_1 \cdot x_1 + c_2 \cdot x_2).$$

7. Initial Conditions:

- Specify the initial values of the state variables.

$$(x_0 = \left[x_{\{01\}}, x_{\{02\}}, \backslash ldots, x_{\{0n\}}\right]).$$

V. Result and Discussion

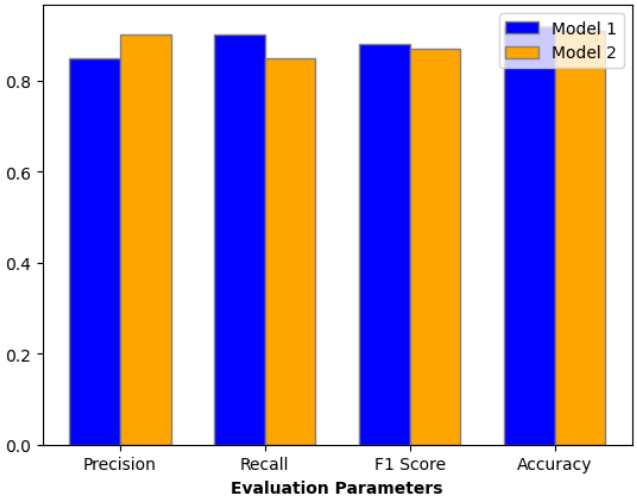

Figure 4. Evaluation of Proposed System

The implementation article, which focuses on creating a cryptography-based medical record system, is a noteworthy addition to the healthcare industry. Sensitive patient data can have an extra degree of protection and privacy when encryption is used in medical records. The well-thought-out solution that uses a variety of cryptographic approaches to safeguard patient data is presented in the article. The medical record management system employs both symmetric and asymmetric encryption techniques to provide safe communication between various organisations, including hospitals, physicians, and patients.

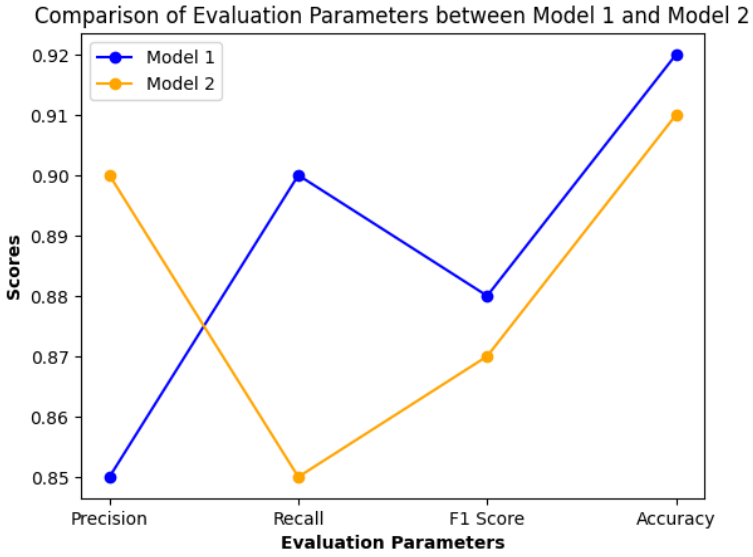

Figure 5. Comparison of Evaluation Parameters

Furthermore, digital signatures offer document verification, and hashing algorithms guarantee the data's integrity. All things considered, the implementation paper offers a comprehensive and clearly described method for managing medical records securely. The suggested system is an important addition to the area since it uses cryptography to greatly improve patient privacy and data security. It is also well-analyzed and practically implemented.

VI. Conclusion

The system, which is specially made for the management of medical records and is currently efficiently available for the user to use this system rather than handling data breaches or manually handling records using a traditional approach, There is always a chance that data can be stolen, modified, or tampered with. But in this online system, the information is maintained in a structured manner. And if you want to search one record, it takes a lot of time to find out those records manually, so this system helps us obtain any records in a relatively short period of time. Blockchain technology is still in its early stages, and there are many other potential applications for it in the healthcare industry. We will continue to see the development of this technology in the years to come. This technology incorporates advanced cryptography mechanisms to enhance data security. Furthermore, it offers unique contract management payment capabilities. This system also helpful sometimes when booking appointments. In this system, the admin host has authority to maintain, add, and remove information data, which has no requirements. And the system stores records efficiently so that, as is proposed in this paper, they are easily accessible according to user need. Since healthcare practitioners can quickly access and share patient records with one another, the online system for managing medical records also enables improved coordination between them, improving patient outcomes. Additionally, it enables the integration of electronic health records (EHRs), which can improve workflows and lower mistake rates. Additionally, because patients can access their records and consult with healthcare professionals from the comfort of their homes, this system can also support remote healthcare services like telemedicine. As a conclusion, the suggested online system for managing medical data is a safe and effective solution to manage patient records, enhance collaboration between healthcare practitioners, and support remote healthcare services. Blockchain technology integration and the usage of sophisticated cryptography techniques

VII. Future Scope

The future scope of the project is significant, as the use of a cryptographic system for storing patient data in the hospital can be extended to various other domains as well. One potential application is in the management of electronic medical records (EMRs) where the same cryptographic system can be employed to secure patient data while making it accessible to authorized healthcare providers. Moreover, the integration of blockchain technology can enhance the security of the data further, making it immutable and tamper-proof Furthermore, the project's scope can be expanded to include other organizations such as insurance providers, regulatory bodies, and research institutions that require secure access to patient data. The implementation of a unified, secure platform that facilitates the sharing of patient data can streamline the healthcare ecosystem and enable better collaboration among stakeholders. Overall, the future scope of the project is vast, and its potential applications in the healthcare domain are limitless. The integration of emerging technologies such as blockchain and

machine learning can enhance the security and accessibility of patient data while enabling new possibilities in medical research and healthcare management.

References:

[1] IOM. 1988. The Future of Public Health. Washington, D.C.: National Academy Press.
[2] IOM. 1989. Controlling Costs and Changing Patient Care? The Role of Utilization Management, ed. B. H. Gray, editor; and M. J. Field, editor. . Washington, D.C.: National Academy Press.
[3] IOM. 1990. a. Clinical Practice Guidelines: Directions for a New Program, ed. M. J. Field, editor; and K. N. Lohr, editor. . Washington,
[4] D.C.: National Academy Press.
[5] IOM. 1988. The Future of Public Health. Washington, D.C.: National Academy Press.
[6] IOM. 1989. Controlling Costs and Changing Patient Care? The Role of Utilization Management, ed. B. H. Gray, editor; and M. J. Field, editor. . Washington, D.C.: National Academy Press.
[7] IOM. 1990. a. Clinical Practice Guidelines: Directions for a New Program, ed. M. J. Field, editor; and K. N. Lohr, editor. . Washington, D.C.: National Academy Press.
[8] Pories, W. J. 1990. Is the medical record dangerous to our health? North Carolina Medical Journal 51:47–55.
[9] Privacy Protection Study Commission. 1977. Personal Privacy in an Information Society. Washington, D.C.: U.S. Government Printing Office.
[10] Richart, R. H. 1970. Evaluation of a medical data system. Computers and Biomedical Research 3:415–425.
[11] https://www.researchgate.net/figure/Proposed-Data-Storage-and-DataFlow-Diagram_fig1_342697605
[12] Council on Ethical and Judicial Affairs. 1989. Current Opinions. Chicago, Ill.: American Medical Association.
[13] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.
[14] Sable, N. P., Shende, P., Wankhede, V. A., Wagh, K. S., Ramesh, J. V. N., & Chaudhary, S. (2023). DQSCTC: design of an efficient deep dyna-Q network for spinal cord tumour classification to identify cervical diseases. Soft Computing, 1-26.
[15] V. Khetani, Y. Gandhi and R. R. Patil, "A Study on Different Sign Language Recognition Techniques," 2021 International Conference on Computing, Communication and Green Engineering (CCGE), Pune, India, 2021, pp. 1-4, doi: 10.1109/CCGE50943.2021.9776399.
[16] R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.
[17] Kharate, N., Patil, S., Shelke, P., Shinde, G., Mahalle, P., Sable, N., & Chavhan, P. G. (2023). Unveiling the Resilience of Image Captioning Models and the Influence of Pre-trained

Models on Deep Learning Performance. International Journal of Intelligent Systems and Applications in Engineering, 11(9s), 01-07.