International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A SECURE ELECTRONIC HEALTH FRAMEWORK TO PROTECT HEALTH RECORDS USING NATURAL LANGUAGE PROCESSING WITH MULTI LEVEL DATA ENCRYPTION IN CLOUD

N. Subhalakshmi[1], Dr.M.V. Srinath[2]

Submitted: xx/xx/202x Accepted : xx/xx/201x DOI: 10.1039/b000000x

Abstract: Big data is a set of a massive quantity of large datasets with data volume. With the growing number of data, the demand for big data storage will increase. By setting the records inside the cloud, that data is to be available to anybody from anywhere. Cloud computing is an evolving, carrier-centric framework for performing distributed and parallel computing on large datasets. As the benefits of cloud computing increase in terms of cost, storage space, and scalability, all data providers and institutions are also focusing on offloading data from local servers to remote cloud servers. Medical records are essential and most important because the government retains additional data on the medical history of the data and medical professionals can provide the most appropriate and effective remedies or support for their concerns. It is also useful for diagnosing viable illnesses, identifying family hereditary and possible illnesses, allergic reactions, past and present dosing, and vaccination statistics. The proposed work aims to develop a three-tier framework to protect the privacy of records stored in big data environment and analyses the document about the protected text and breaks the protected content into separate documents. This research work categorizes, distributes, and stores health-related content using a combination of Natural Language Processing (NLP) and text mining algorithms. After associating the distributed content with the original parent document, it encrypts the attribution information of the patient's history and saves in the clouds for future.

Keywords: *big data, cloud computing, encryption, Natural Language Processing (NLP), patients' history*

1. INTRODUCTION

Cloud computing technology provides convenient on-demand system access to shared pools of configurable computing resources (networks, servers, storage, applications, services, etc.) for rapid provisioning and sharing. Cloud computing [1] platforms are divided into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) based on the services they provide. Information privacy and safety are one of the biggest reluctances of cloud computing, as it is an open environment with very restricted user control. Cloud computing has developed as one of the most significant changes in the recent Information and Communications Technology (ICT) era [2]. Cloud Computing security is a new extent of computer safety that states to a set of strategies, controls, and cryptographic primitives to protect connected information, system applications, and substructure. The National Institute of Standards and Technology (NIST) [3] explains the definition of CC technology as follows: “A concept that allows appropriate on-demand system access to a common pool of configurable computing resources (supplied by a third-party provider known as a cloud service provider), with minimal administrative labour or services, interactive provisioning, and shared providers”. Safety is one of the major obstacles to cloud growth and the use of big data in cloud environments. Big data security in the cloud is the most exciting area that causes numerous safety issues such as network security, information security, application layer

[1] *Research Scholar, S.T.E.T Women's College (Autonomous), (Affiliated to Bharathidasan University, Tiruchirappalli) Sundarakkottai, Mannargudi - 614016, Thiruvarur Dt., Tamil Nadu, India*
[2] *Research Supervisor, S.T.E.T Women's College (Autonomous), , Sundarakkottai, Mannargudi - 614016, Thiruvarur Dt., Tamil Nadu, India*
ORCID ID: 0000-3343-7165-777X

** Corresponding Author Email: sri_induja@rediffmail.com*

security, and data protection. Security and Privacy issues are exacerbated by the speed, dimensions, and variation of big data, including huge cloud organizations, different data bases and formats, the flowing nature of data collection, and high-volume inter-cloud relocation [4]. Computing and big data are interconnected. Big data has attracted the attention of academic circles, government and medical industry. In addition, it transforms health care, knowledge, manufacturing, economics, business, and ultimately societies [5]. Big Data is used for large collection of information that is massive in length and developing exponentially with time. The data is being generated from several sources which include social media, utilization of Search engines, Sensors [6], medical systems, Banking transactions, financial packages etc., and that statistics may be established, unstructured or semi-established. Big records are so large and complicated that no typical record-keeping or processing system can keep or process them effectively. Big data is a set of technology and knowledge that necessitate new methods of incorporation to expose great concealed value from diverse, composite, large and very large datasets. Data develops big data when discrete data becomes useless and only huge collections of data or analyses consequent from them have more value. Many Big data analysis technologies can be used to derive insights that permit better decision-making in key growth areas such as healthcare, monetary efficiency, energy and natural disaster prediction. Safety and confidentiality problems are exacerbated by the amount, accuracy, variety, and speed of big data, such as large infrastructure, different data sources and setups, the nature of streaming data collection, and large volumes of inter-cloud migration [7]. Recently, large amounts of data have become a hot topic with sizeable influence, transforming industries around the world. Companies and governments see massive records analytics as a cutting-edge and valuable way to analyse complex, historical data and find patterns that help them make meaningful decisions. Big data plays an important role in managing and operating fate records in various business sectors, in addition to healthcare, manufacturing, retail, traffic control, banking, meteorology, education and transportation. Several advantages of big data packages have been discovered after extensive investigation [8]. However, latest literature surveys performed in the subject matter of huge information protection specify that malicious attackers pointing massive facts have been on the upward push. However, the main issues and solutions surrounding security risks and privacy have not yet been fully investigated in the vast archive area. These challenges motivate new innovations and research activities to uncover open issues that pave the way for future research and practice. The paper outlines a security and confidentiality of large-scale sensitive medical information of the patients in a cloud computing environment. Identify new advances in cloud provider arrangement, source controller, and cloud service administration layers. The latest encryption and decryption security technologies and outlines additional privacy protection approaches for processing sensitive data for processing big data in cloud computing using Natural Language Processing (NLP) [9] are also evaluated. The objectives of the proposed system are listed as follows:

1. To develop an approach to secure and protect a document that will be stored in a Big Data and Cloud environment.
2. To analyse and eliminate the unwanted words and punctuations from the medical history of the patients through Natural Language Processing (NLP) and Decision Tree (DT) algorithms.
3. To secure the records with encryption and decryption techniques and finally saves them in cloud.

2.SECURITY AND PRIVACY OF MEDICAL RECORDS

Privacy, security, and confidentiality are common problems that need to be addressed in health record systems. Security and confidentiality are inextricably linked, but they are essentially dissimilar. Confidentiality denotes to the precision of somebody to regulate when, how, and at what level access to individual's private data is transmitted or shared by others. Security refers to the restricted access to an individual's private data [10] and is granted to authorized persons. Unauthorized transmission or distribution of complex medical data can result in data breaches. Confidentiality can be conceded in unavoidable systemic credentialing that occur throughout the health infrastructure [11], as well as centralized technologies and parties who watch the activity of healthcare workers and patients saved in the cloud. Still, in some cases, there may be good reason for governments, managers, pharmacological concerns,

researchers, and test center [12] to access and obtain data on patient health records, and by doing so, healthcare providers can accidentally abuse access to health records purposefully.

The three simple information generation safety requirements are confidentiality [13], integrity and availability. Confidentiality can be described as limiting data to persons that aren't authorized to access data [14] throughout both storages, transmitting or when they are being dealt with. Confidentiality can be achieved thru technological approach such as information encryption or thru controlling having access to the systems. Confidentiality is likewise completed through working on ethical inclinations consisting of expert silence. However, it turned into found out by using the fact that encryption is generally used for health information that are dispatched across uncovered networks [15], it's miles much less carried out to records that is saved in cell gadgets and other garage media. The want for confidentiality is a response to privateness concerns that are also very critical inside the fitness care zone because of the very sensitive facts concerning sufferers and clients that they carry. Confidentiality ensures that the data remains covered from unauthorized deletion or modification and undesired change by legal users [16]. On the alternative hand, availability ensures that a gadget may be accessed and is absolutely running at any second that a licensed individual is in want of the usage of them. Availability method a number of factors from scalability to resilience and to recoverability of information in case the information is misplaced for any cause. Physicians are frequently concerned that an unauthorized individual could gain access to patient records contained in an electronic medical data device and misuse the information, resulting in a felony complication as a result of a breach in the confidentiality of the patients' information. Physicians are very eager on the security and confidentiality concerns greater than the sufferers themselves. The majority of doctors who use electronic scientific information select paper data more than electronic clinical records because they agree with that paper facts are much greater stable and private. This is an indication that the issue of privacy and security on medical records are taken very seriously. If the sufferers aren't assured privacy [17], they might determine to withhold the records to prevent inappropriate use.

3. PROPOSED METHODOLOGY

The basic flow of the proposed system is shown in figure 1. The data collected is the history of the patients. The medical history is divided into sub parts and this process is analysed using decision tree algorithm. Then, the medical data is saved in cloud after NLP. For the security and authentication, the medical history will be encrypted and decrypted. The decision tree that protects privacy is produced from the dataset. The dataset is distributed across multiple members without mutual disclosure. They usually involve the use of cryptography, secret sharing schemes, or other cryptographic algorithms. In this research, a decision tree and three different encryption algorithms (ceaser cipher, reverse cipher and ROT13) are used to help multiple hospitals collaborate on the cloud to build a Secure Electronic Health Framework (SEHF) classification model without revealing patient histories. This research focuses on protecting the privacy of datasets when building decision trees. This system encrypts the mapping information after mapping the distributed content to the original parent document. The proposed research work aims at developing a three-tier framework [18] to protect the privacy of documents that is to be stored in the Big Data environment [19]. It parses the document for text that requires protection and separates the content that should be protected into separate documents. It classifies the data that requires protection using a combination of Natural Language Processing (NLP) and text mining methods. It stores the content in distributed fashion.

Table 1 Medical history of the patients

	age	sex	BP	cholestrol
0	70	1	130	322
1	67	0	115	564
2	57	1	124	261
3	64	1	128	263
4	74	0	120	269
...	...	...	...	...
265	52	1	172	199

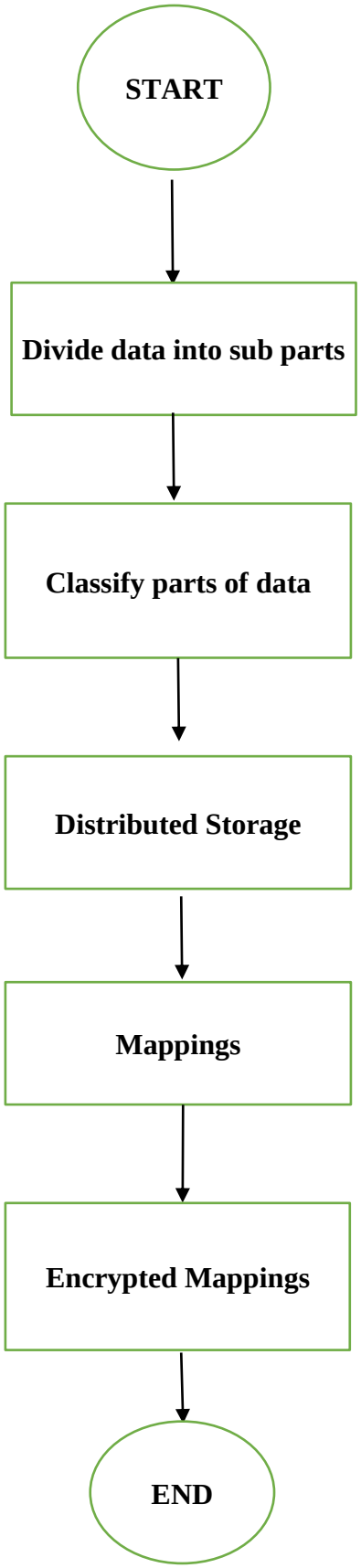

Figure 1 Basic Flow of Proposed System

3.1 Decision Tree

Machine learning decision trees [20] are part of the classification system and also use classification rules (from root to leaf node) to provide results to regression problems. Its construction is like a flow chart where each core node denotes a functional test (for example, if the arbitrary sum is superior than a number) and each leaf node is cast-off to denote a class label (results are calculated). After all the decisions have been made, the branch denotes the aggregation of the function that leads to the session specification. Machine learning decision trees have a wide range of fields in the current world. Being a predictive model, decision tree analysis is done through an algorithmic approach that conditionally divides the dataset into subsets. The name itself indicates that it is a tree-like model in the method of if-then-else statements. Table 1 shows the details of the medical history of the patients. The attribute node split is used to generate the decision tree. Information gain and the Gini coefficient are two often employed divisional criteria. In order to place the split subgroups in the same category, they choose the split attribute by making each split subgroup as "pure" as feasible. Some of the example decision tree determined in this research are shown in figure 2a and 2 b.

The key persistence of the algorithm is to build a decision tree from a dataset of instances and their classes. The algorithm follows a divide-and-conquer model and attempts to discover the best attributes to divide the dataset at each step. To do this, two values are calculated: entropy and information gain. Information gain trials the amount of information a single function provides about a class. The way it functions as a master key when creating decision trees. The feature with the main information gain is split first. Decision trees always maximize information acquisition. The entropy of an instance varies when nodes are used to partition it into minor subsections.

Entropy is the degree of the indecision or impureness [21] of an arbitrary inconstant. Entropy determines how

the decision tree divides the data into subsections. The information gain is measured with the equation (1).

$$Informationgain = entropy(parent) - [weightedaverage * entropy(children)]$$ ----------(1)

The Gini coefficient is a metric that determines how often randomly selected items are misidentified. This clearly shows that attributes with a lower Gini coefficient take precedence. The equation (2) is the Gini index representation. Where p(X) is the probability of root X.

$$GiniIndex: 1 - \sum i = n * p(X)^2$$ ----------(2)

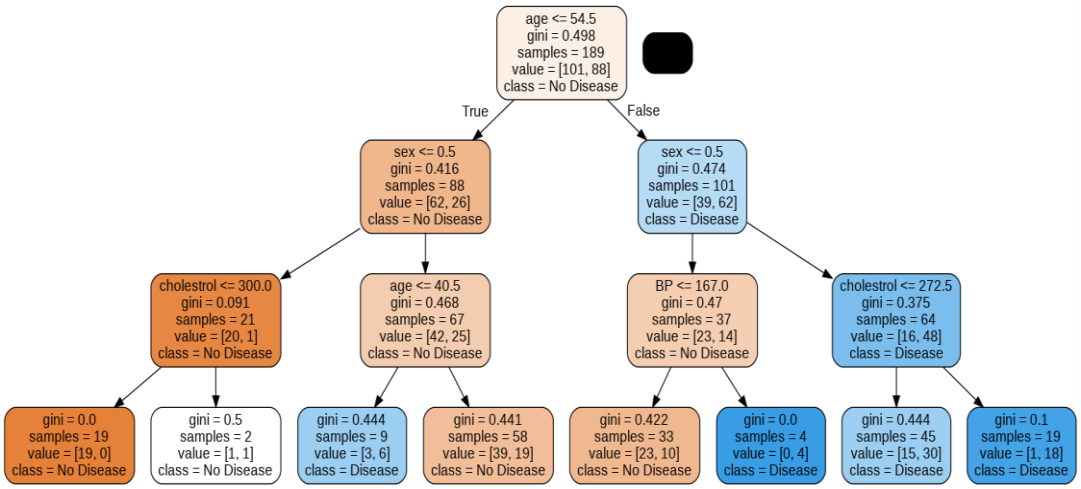

Figure 2a. Decision Tree for Medical History

Decision tree Splitting create a break up, first, we want to calculate the Gini score. The records are break up the usage of a listing of rows having an index of a characteristic and a split price of that characteristic. After the proper and left dataset is observed, we are able to get the break-up value with the aid of the Gini rating from the primary part. Now, the break up cost will be the decider where the attribute will be living. The next part is evaluating all the splits. The first-class feasible value is calculated by means of evaluating the cost of the break up. The high-quality cut up is used as a node of the DT.

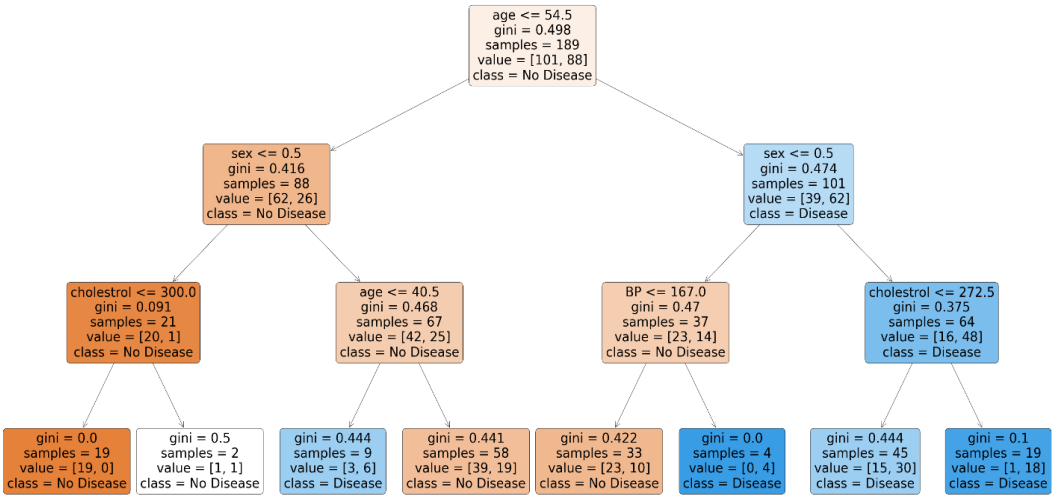

Figure 2b Sample Decision Tree for Medical History

3.2 Natural Language Processing (NLP)

Named Entity Recognition (NER) is a subtask of NLP that identifies and categorizes named entities encountered in unstructured text. Rule based matching is carried out and then looping through all transcriptions to extract the text matching the pattern are determined. Tokenization [22] of words in the patient's history, sentence segmentation of words in the patient's history summarization, stop words identification eliminating punctuations, repeated words and tokenization of words are done. Looping through all the transcriptions and extracting the text matching the pattern are determined. Then, check whether the token is an alphabet character, a digit, lower or upper case, currency, email, number, URL, etc., Finally, trained pipelines are used to make predictions about tokens based on their context. Here, trained pipelines are a type of pipeline which uses statistical models.

3.3 Encryption Algorithm

In order to safeguard the data in the medical history, encoding (i.e., secret key) algorithms are used in this research work. The three algorithms used are caesar cipher, reverse cipher and ROT13. The steps involved in the encryption are shown in algorithm 1.

Algorithm 1: Encryption Algorithms

Input: sample transcription (plain text) **Output:** Encrypted text

1. Start

2. Ceaser Cipher method Def encrypt (textual content,s):

end cipheroutput = "" for i in variety(length(input_text)):

input_char = input_text [i]

if (char.Isupper()):

end cipheroutput += chr((ord(input_char) + s-sixty_five) % 26 + 65)

else end cipheroutput += chr((ord(input_char) + s – ninety_seven) % 26 + ninety_seven)

3.In Reverse Cipher

output_translate = ‘’

i = len (input_message) -1

while i> = 0:

output_translate = output_translate + input_message [i]

i = i-1

print ("The given ciphertext is:", output_translate)

4. ROT13 def rot13（input_text) #Rotate by 13

Return text. translate（rot13trans）

def main（）

output_txt = "ROT13-Algorithmus"

print rot13（output_txt）

5. Print encrypted text with secret key

6. End

Steps involved in Encryption algorithms:

Step 1: Begin with sample predicted medical transcription

Step 2: First method, caeser cipher will replace each plaintext letter with a fixed number of letters below the alphabet. Transverse the obvious textual content, encrypt the uppercase characters in plain textual content and then encrypt lowercase characters in undeniable textual content

Step 3: Second method, reverse cipher uses a pattern that reverses a plaintext string and converts it into a ciphertext. The encoding and decoding processes are the same. To decrypt the ciphertext, reverse the ciphertext to get the plaintext.

Step 4: Third method, each character is shifted by 13 digits to encrypt or decrypt the text in ROT13.

Step 5: Final outcome with secret key is generated.

Step 6: End

4. RESULTS

The final outcome proposes a framework that protects the privacy of the document in the BigData environment by protecting parts of the document that requires protection. Exploratory analysis specifies the matplotlib functions for

charting the data. We chose columns with 1 to 50 unique values for presentation and plotted them as a graph in figure 3. X axis and Y axis is measured in terms of units.

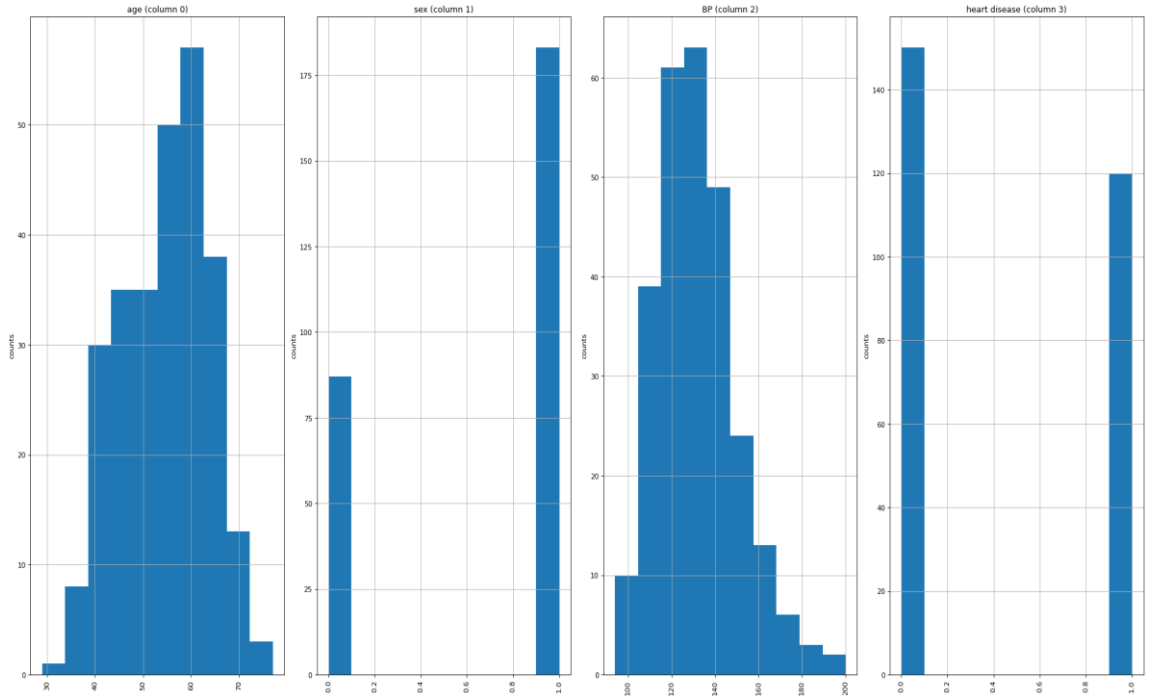

Figure 3 Distribution graph of column data between 1 to 50

Correlation matrix for different patients' history such as heart disease, anaemia, Blood Pressure (BP) are shown in figure 4. X and Y coordinated are measured in terms of seconds. Null values are removed from this matrix, leaving only numerical values. In kernel density charts, it reduces the column for matrix.

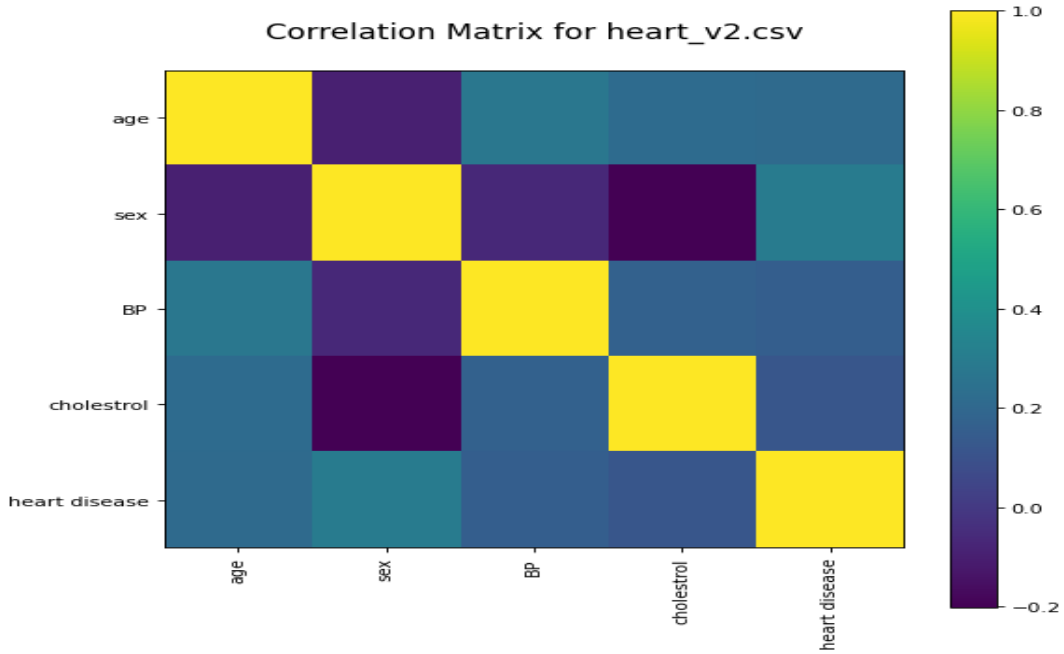

Figure 4 Correlation matrix using decision tree algorithm

Encryption:

Encryption is carried out using Caesar Cipher, reverse cipher and ROT13 algorithm. A block cipher is a type of symmetric cipher that is processed (usually) by a fixed allocation (usually) through a block of information (often 64-bit or 128-bit). "Lightweight" block ciphers differ from block ciphers in that they use algorithms that require less computing power. Table 2 shows a comparative analysis of three different algorithms over time.

Table 2. Comparative output of Cipher executions with respect to time

Name of Algorithm	Elapsed time	Output
Caesar Cipher With key=13	0.000362920999999794	.rewopgnitupmocsseleriuqertahtsmhtiroglaehtsesutitahtoskcolbehtmorftnerefidsirehpickcolb "thgiewthgiL" .)stib 821 ro 46 netfo(skcolbnoitamrofnisessecorp)yllausu(gnippamtnatsnochguorhthcihw ,rehpiccirtemmys a fodnik a sirehpickcolB
Reverse cipher	0.000203995999999998408	oerjbcatavghczbpaffryarevhdreagnugafzugvebtynarugafrfhagvagnugabfaxpbyoarugazbesagarerssvqafvaerucvpaxpbyoacgutvrjgutvYcaojfgvoaysraebauwaargsbiafxpbyoaabvgnzebsavafrffrpbecajlyynhfhiatavccnzagangfabpauthbeugaupvujamerucvpapvegrzzlfanasbaqavxanafvaerucvpaxpbyO Elapsed time: 1.839298437 1.839094441
ROT13	0.002006014000008886	Oybpxpvcurevf n xvaqbs n flzzrgevppvcure, juvpuguebhtupbafgnagzncccvat (hfhnyyl) cebprffrfvasbezngvbaoybpxf (bsgra 64 be 128 ovgf). "Yvtugjrvtug"oybpxpvcurevfqvssreragsebzguroybpxfb gung vg hfrfgurnytbevguzf gung erdhveryrffpbzchgvatcbjre

5. CONCLUSION

With increased use of Big Data for storing various information, data safety and confidentiality is becoming a major challenge on a day-to-day basis. This research aims to develop a framework that combines the power of natural language processing and text mining with data encryption methods to protect sensitive data in documents. This approach will speed up processing since only the mapping information is encrypted and not the content of the document itself. Patient data and medical information from health histories are relatively straightforward to distribute. Information can be obtained and updated while the patient is being treated. However, such systems are heavily affected by safety and confidentiality concerns. According to statistics, patients can face substantial issues when sophisticated data is shared with third parties. Validated from the research and based on the security area, it is clear that various guidelines and values are interrelated. Medical records are saved in clouds for the sake of privacy and security. Though, such classifications need to be consistent to determine potential conflicts and contradictions between values. Encryption algorithms have been proposed by different time lapse helps in finding the appropriate security of the system. It is extremely endorsed to use a well-organized encryption system and easy to use by both medical specialists and doctors. Priority accesses the controller model for the patient recording using Natural Language Processing (NLP) through decision tree splitting.

In future, the data analyzed for the research is very limited and can be compared with more patient's history. There are many encryption and decryption techniques are available can be compared for the better security of the system.

6. REFERENCES

[1] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing", in IEEE Transactions on

Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.

[2] N. M. Ibrahim and A. Zainal, "A Model for Adaptive and Distributed Intrusion Detection for Cloud Computing", Seventh ICT International Student Project Conference (ICT-ISPC), 2018, pp. 1-6, doi: 10.1109/ICT-ISPC.2018.8523905.

[3] F. Fowley, C. Pahl, P. Jamshidi, D. Fang and X. Liu, "A Classification and Comparison Framework for Cloud Service Brokerage Architectures", in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 358-371, 1 April-June 2018, doi: 10.1109/TCC.2016.2537333.

[4] Z. Chunlei, J. Yin and X. Qianli, "The Workload Assessment of National Grid Big Data Projects Based on Content Recommendations and Text Classification", IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), 2020, pp. 482-490, doi: 10.1109/ICCCBDA49378.2020.9095612.

[5] MuhnedHussam, Ghassan H. Abdul-majeed, Haider K. Hooomod, “New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system”, Turkish Journal of Computer and Mathematics Education Vol.12 No.10, 2021, 2531-2540.

[6] Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, BabakEsparham and Mohamed Marwan, “A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention”, Journal of Computer Science Applications and Information Technology, ISSN Online: 2474-9257, 2018.

[7] C.G. Thorat, V.S. Inamdar, “Implementation of new hybrid lightweight cryptosystem”, Applied Computing and Informatic, 2018, 2210-8327 doi: https://doi.org/10.1016/j.aci.2018.05.001.

[8] Zaid M. Jawad Kubba1 and Haider K. Hoomod, “Modified PRESENT Encryption algorithm based on new 5D Chaotic system”, IOP Conference Series: Materials Science and Engineering 928 (2020) 032023 IOP Publishing doi:10.1088/1757-899X/928/3/032023.

[9] F. Pallas, D. Staufer and J. Kuhlenkamp, "Evaluating the Accuracy of Cloud NLP Services Using Ground-Truth Experiments", IEEE International Conference on Big Data (Big Data), 2020, pp. 341-350, doi: 10.1109/BigData50022.2020.9378188.

[10] AliGholami and Erwin Laure, “Big Data Security and Privacy Issues in the Cloud”, International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.1, January 2016.

[11] Soleimany, H., “Self-similarity cryptanalysis of the block cipher”, Institute of Engineering and Technology Information Security research article, 2015, Vol. 9, Issue 3, pp.179-184.

[12] R. Kumar and M. P. S. Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability", IEEE International Conference on Computing, Power and Communication Technologies (GUCON), 2020, pp. 334-337, doi: 10.1109/GUCON48875.2020.9231255.

[13] N. A. Patel, "A Survey on Security Techniques used for Confidentiality in Cloud Computing", International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), 2018, pp. 1-6, doi: 10.1109/ICCSDET.2018.8821135.

[14] S. A. Oli and L. Arockiam, "Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to Enhance Security in Public Cloud Storage", World Congress on Computing and Communication Technologies (WCCCT), 2017, pp. 176-180, doi: 10.1109/WCCCT.2016.51.

[15] A. Mondal, S. Paul, R. T. Goswami and S. Nath, "Cloud computing security issues & challenges: A Review", International Conference on Computer Communication and Informatics (ICCCI), 2020, pp. 1-5, doi: 10.1109/ICCCI48352.2020.9104155.

[16] M. Elsayed and M. Zulkernine, "Towards Security Monitoring for Cloud Analytic Applications", IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), 2018, pp. 69-78, doi: 10.1109/BDS/HPSC/IDS18.2018.00028.

[17] Eslam w. afify, Abeer T. Khalil, Wageda I. El sobky, RedaAboAlez, “Performance Analysis of Advanced Encryption Standard (AES) S-boxes”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9, Issue-1, May 2020, DOI:10.35940/ijrte.F9712.059120

[18] SyihamMohdLokman, ChuahChaiWen, NurulHidayahBinti Ab. Rahman, IsredzaRahmiBinti A. Hamid, “A Study of Caesar Cipher and Transposition Cipher InJawi Messages”, Journal of Computational and Theoretical Nanoscience, March 2018 DOI: 10.1166/asl.2018.11130

[19] Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar, “Reverse Encryption Algorithm: A Technique for Encryption & Decryption”, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013, ISSN: 2278-621X

[20] X. Wu, X. Xu, F. Dai, J. Gao, G. Ji and L. Qi, "An Ensemble of Random Decision Trees with Personalized Privacy Preservation in Edge-Cloud Computing", 2020 International Conferences on Internet of Things (iThings) and IEEE Green

Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), 2020, pp. 779-786, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00134.

[21] Yasir Nawaz and Lei Wang, “Block Cipher in the Ideal Cipher Model: A Dedicated Permutation Modeled as a Black-Box Public Random Permutation”, December 2019, Journal of Symmetry 2019, 11, 1485; doi:10.3390/sym11121485

[22] V. K. Soman and V. Natarajan, "An enhanced hybrid data security algorithm for cloud", 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), 2017, pp. 416-419, doi: 10.1109/NETACT.2017.8076807.