A Novel medical data privacy model using IoT Data for Multi Keyword Search using N-Gram block chain Algorithm

[1]**J.N.S.S Janardhana Naidu**, Department of CSE Vels Institute of Science Technology and Advanced Studies**,** **jnss.janardhana@gmail.com**

[2]**Dr.E.N.Ganesh**, Vels Institute of Science Technology and Advanced Studies Professor, Dean School of Engineering VISTAS**,** dean.se@velsuniv.ac.in **,** enganesh50@gmail.com

Abstract

For more choice and financial speculation reserves, dispersed processing allows data proprietors to reorganize their medical records from nearby locations into the open IoT network. In any case, sensitive data should be encoded before being re-distributed for the sake of monitoring estimations security, which replaces the usual practice of using plaintext keyword search. As a result, allowing for the search for organization of encrypted IoT data documents is critical. A few key words in the search for stores and return records may go a long way toward determining whether or not they are relevant to these important articulations, especially when considering the enormous amount of data customers and documents save in the IoT network. On a single catchphrase search or Boolean watchword look for, this method wears out open encryption thinking. In this research, for the first time, graph and deal with the bothersome problem of privately shielding multiple catchphrases placed in the investigation of encoded substances in transmission processing (MRSE). We created a private company to meet the needs of this IoT information usage contraption's severe privacy requirements. In this choose the green similarity dimension of "organise planning," i.e., as many suits as are feasible, from among the various multi-watchword semantics, in order to get the congruity of records reports with respect to the mission issue. In addition, employ "inward thing likeness" to look at such similarity in quantitative terms. When it comes to managing risk in our industry, first have to figure out what we're dealing with, and then have to figure out what we're dealing with in terms of how we're dealing with it. In addition to enhancing those designs to assist with more significant request semantics with N-gram block chain capabilities, enhance the recognition of records look transporter to better look.

Keywords: IoT registering, counter-intelligence, out-sourced information, protection, likeness look.

1. Introduction

Because of the rapid development of records, experience owners will preserve their realities on the IoT to alleviate the burden of estimates storage and security. Our reappropriated experiences, however, may be under the consideration of probability due to their not being in the same dependent district as the IoT clients and IoT server. As a result, before to being

transferred to the IoT, the calculations must be encoded to protect private information and prevent unrestricted access. It's a shame that the traditional plaintext look frameworks can no longer be quickly implemented to the mixed IoT data. Traditional data recovery (IR) has lately offered the information consumer access to multi-catchphrase-based queries. As guarded substances and security searches are conducted in an ambiguous manner, the IoT server must provide the records client with a corresponding restriction. Securing it on a IoT server is a cinch since sureness's can be found and used with ease.

Encryption frameworks that are accessible in the composition may provide consumers with aesthetically beautiful encoded data. It's made up of an open-ended document that provides a quick look at the mapping between watchwords and the corresponding collection of data. An entry point is provided for the keyword by the IoT server, and a few professionals do study on the subject using an attractive and well-placed search across dispersed IoT pieces of information. advocate a catchphrase look plan that is well-placed. Changed records and solicitation-free symmetric encryption are combined in their response (OPSE). It is possible that the method for TFIDF will govern the selection of recouped documents in articulations of placed look. Security measures for OPSE have a significant impact on the importance score. It enhances the use of the gadgets, as well as the amount of noise they make. This solution only works with a single-word search. According to Cao et al. they've discovered a method for measuring the "mastermind planning" equivalency in terms of the request's relevance. In order to rate each report, they employ "internal thing likeness." This strategy aids in the search for genuine multi-watchword positions. It's logical yet the pursuit is wacky at the same time. Situated keyword search is supported by Sun et al. MDB-tree based organisation. Even though this arrangement is feasible, a superior execution will result in a reduction in the exactness of the pursuit consequences.

Further, a cushioning search was carried out. Using a spellcheck framework, these methods search for "r" "Instead of "wireless," you may want to use "mote" or "wireless," since the records setup may not be the same. By way of example, Chuahet al., provide an assurance aware bed tree strategy to aid fleecy multi-concept look. To produce feathery watchword units, this technique makes advantage of change division. Every catchphrase has its own Bloom channel. By this time, it has built up a record tree for all reports in which each leaf centre marks a hash cost of a keyword. It is possible to generate storage-efficient padded catchphrase units by using the modified division technique of Li et al. It is intended to minimize overhead by using a trump card-based, fully cushioned set-age technique. Wang and colleagues choose a trump card-based feathery set to build a tire-explore that is not available to the outside world. It's considered comparable and re-establishes the corresponding reports if the change expulsion between recovery catchphrases and ones from the rough units isn't precisely a fixed set esteem in the looking component. However, they do not foster semantic feathery search, these cosy search philosophies serve to counter teenage blunders and inappropriate associations. Multi-catchphrase located search and semantic search for are becoming more and more reasonable given the prevalence of polysemy and synonymy.

Multi-keyword idle semantic situated investigation encoded IoT substances may be fixed in this article and the most significant records recovered. Multi-catchphrase inactive semantic situated look for Latent Semantic Appraisal (LSA)-based multi-catchphrase situated look is another arrangement that we outline. LSA-based technique may need restoring more than just exact organizational reports; it may also necessitate restoring data that includes torpid semantically recognized articulations associated with the request keyword. According to the suggested system's design, when a client enters the catchphrase "vehicle" to search for records, it returns not only records containing "vehicle," but also the papers that include "vehicle." It is possible to assemble a semantic zone where articulations and recordings that are enthusiastically associated are located near to each other in a huge system of time span report alliance pieces of information The notion of a multi-catchphrase located search for (MRSE) the use of is one we suggest to meet the need of enabling such multi-watchword semantic without privacy breaches "Foreground Semantic evaluation

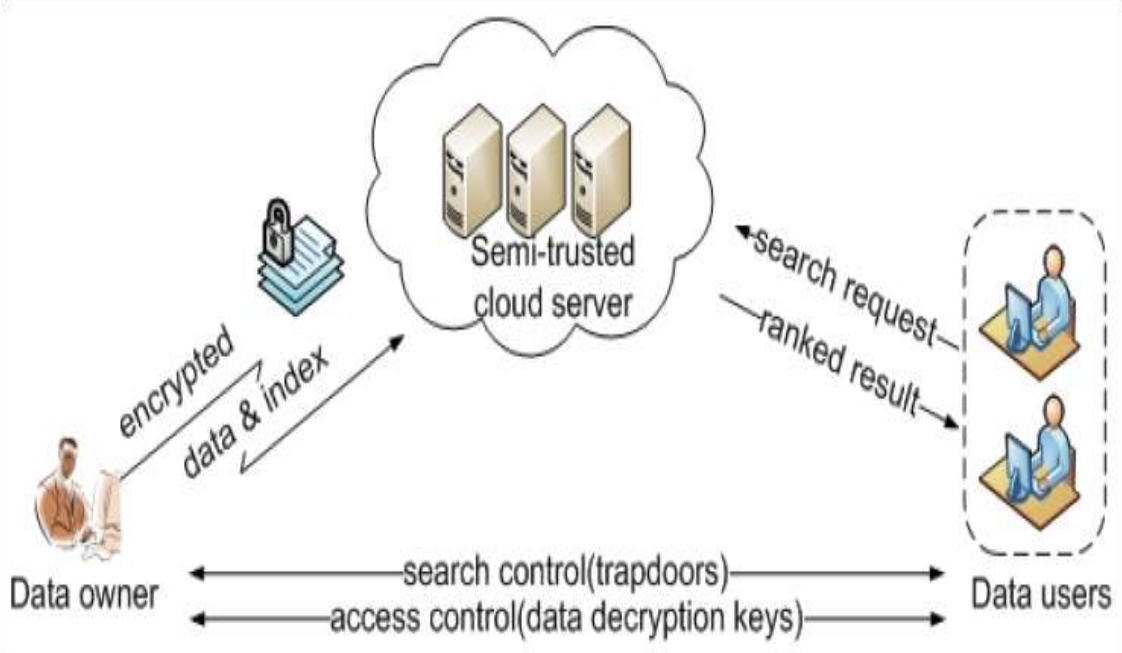

Figure 1: architecture

2. Literature Survey

Jaikar, A.,et al [2017] Retrieval methods play a critical role in the information age. One method of retrieving data associated with a certain term is the inverted index. Using this method, you may quickly find the appropriate document among the billions of papers that include the term you provide. Many strategies have been suggested to accommodate incorrectly spelt keywords, such as edit distance, wildcards, and n-grams block chain. A benefit of the n-gram index is that it is language-independent and error-tolerant. Nevertheless, its bulk and lower performance limit its usefulness. In this study, we've developed a novel

method for searching for fuzzy terms. The suggested method has been built and evaluated on two datasets. NOVEL approach not only accommodates misspelt terms but also reduces the size of the gramme by 40-50 percent compared to K/n-gram technique, as shown in the results. Therefore, the suggested method is the most effective method for supporting fuzzy keyword search.[1]

Fan, K.,et al [2017] When it comes to protecting sensitive information in large data, IoT storage is becoming more and more popular. Security and privacy of the stored data are major considerations when using a IoT server since the server itself might leak information. As a result, before being moved to the IoT, critical data must be encrypted. Authorized users will appreciate how easy it is to do a keyword search to access encrypted data from the IoT. It is well-known that re-retrieving all documents that match a query is inefficient. Fuzzy multi-keyword search may be supported by certain techniques, however they are usually dependent on edit distance to hunt for a set of fuzzy alternatives, which results in a substantially bigger index file and a more complicated query. The search results are then sorted based on how closely the keywords and documents match. A new multi-keyword fuzzy and sortable search method is presented in this study. Fuzzy search is made possible by the use of n-gram technology, and we provide a new ranking method for fuzzy multi-keyword searches. There are discrepancies between the original query keywords and the fuzzy keywords since there may be more than one matched file. In addition to the relevance score between the index keywords and the documents, the similarity between the query and keywords will be taken into account when ranking files. As a result, we generate the file's full matching score, which is more accurate and efficient.[2]

Wang, H.,et al [2020] Natural language processing (NLP) applications rely on text categorization as a foundational function. While the majority of prior research has focused on either explicit or implicit text representation to solve this sort of issue, both strategies work well for sentences and can't easily be applied to short text due of its brevity and sparseness features. According to these facts, we propose a new kind of short text classification model using CNN, which can get the abundant text feature by adopting none linear sliding method and N-gram language model, and picks out the key features using the concentration mechanism, in ad nauseum For the brief text classification, an experiment reveals that our technique, compared to the classic machine learning algorithm and convolutional neural network, may significantly enhance classification results.[3]

Kaur, S.,et al [2018] Any text may be subjected to a sentiment analysis to determine its positive, negative, or neutral qualities. In the last several years, a variety of methods have been developed for analysing the sentiment of tweets. According to past research on sentiment analysis, a unique technique to sentiment analysis of Twitter data is described in this research article. Feature extraction and classification methods are combined in the suggested method. The KNN classifier is used to categorise input data into positive, negative, and neutral categories using the N-gram technique. Precision, recall, and accuracy are three

metrics used to evaluate the proposed system's performance. As a comparison to SVM-based classification, the experimental findings suggest that the proposed system outperforms it.[4]

Violos, J.,et al [2018] Classification of high-frequency data streams is a major issue in today's information era. It is proposed in this study to develop an elastic distributed text stream classification model that can handle a fluctuating text load while still being novel and accurate. Text is represented as N-Gram Graphs in this classification model, and the classification process is carried out utilising text pre-processing, graph similarity, and feature classification approaches. Many different models and parameter combinations are examined in order to arrive at the most accurate set-up, including diverse text representations like N-Gram Graphs, graph comparison metrics, and classification algorithms. The Beam programming approach is used to cope with the scalability, availability, and rapid reaction to high frequency text. The inference stage's most computationally intensive activities may be dispersed over a distributed computing environment using the Beam programming paradigm. High-frequency streams are simulated using two datasets (20NewsGroup and Reuters-21578) extensively used in the literature for text categorization. The suggested model and its different parameters have been tested experimentally.[5]

Ali, M.,et al [2020] Modern malware detection and mitigation are essential for a company's smooth functioning. By using methods like code obfuscation, metamorphism, and polymorphism, attackers may make malware more resilient than traditional defences can. Protecting IT infrastructure from such assaults and guaranteeing its security are both pressing needs that can only be solved by developing adaptive, more effective malware detection techniques. Using N-grams and machine learning, we examine an alternate way for detecting malware. We extract an Indicator of Compromise (IOC) for malicious files that are represented using N-grams utilising a dynamic analysis approach. For the purpose of inputting the most important N-grams characteristics into a machine learning algorithm, the authors provide TF-IDF as a new method of doing so. Finally, multiple supervised machine-learning techniques are used to assess the suggested approach. When compared to the other classifiers, Logistic Regression has the greatest classification accuracy with a score of 98.4%[6]

Peng, J.,et al [2016] A wide range of data is provided by users when they engage with social media, from ratings and approvals to the amount of text they post. Many of the contributions to public discussions about hotspots may be traced back to a specific user identification or nom de plume. Using n-gram analysis on the bit-level rendering of the text, it may be possible to detect the authorship of distinct tracts of text on social media. For the purpose of identifying the authorship of two months' worth of user comments from a news and opinion website with moderated debate, this article uses bit-level n-gram analysis in conjunction with other statistical classification methodologies. The findings suggest that this strategy can obtain a high recognition rate with a low percentage of false negatives,[7]

Chen, J.,et al [2017] Increasingly popular are keyword searches over encrypted IoT data, prompted by privacy concerns over outsourcing data. Multi-keyword fuzzy search techniques are more popular than single-keyword precise searches because they enhance search accuracy, typo tolerance, and overall user experience. As a result, conventional multi-keyword fuzzy search techniques are ineffective when the IoT file set is quite vast. An Efficient Leakage-resistant Multi-keyword Fuzzy Search (EliMFS) architecture for encrypted IoT data is proposed to solve this issue Search time is unaffected by the size of a file set in this framework because of a two-stage index structure. Based on Gram Counting Order, Bloom filter, and Locality-Sensitive Hashing, the multi-keyword fuzzy search function is realised. In addition, we present two particular techniques to protect against leaks produced by the two-stage index structure in various threat models. Our systems have been thoroughly tested and shown to be leakage-resistant and extremely efficient.[8]

Liu, D.,et al [2018] Numerous problems have been found and real-world situations replicated through crowdsourced software testing. As a result, it is widely used in mobile app testing. Mobile testing, on the other hand, often simply includes a few screenshots and a few sentences of text as the report's body. It's a time-consuming yet necessary effort to review and understand the vast quantity of mobile crowdsourcing test results. New techniques to help developers interpret crowdsourced test results are motivated by the lack of textual information and the well-defined images of activity views in mobile apps. In this research, we offer a completely automated method for generating descriptive phrases for well-defined screenshots. To create language models, we rely on the results of tests conducted by qualified testers. Spatial Pyramid Matching (SPM) is a computer vision algorithm that measures and extracts characteristics from screenshot pictures based on similarities. More than 1000 test reports from four industrial crowdsourcing projects suggest that our proposed approach is promising for developers to better comprehend the mobile crowdsourced test reports..[9]

Guha, A.,ET AL [2021] In the last twenty-five to thirty years, the Internet has fundamentally altered almost every business paradigm in existence. Data digitization and management has been revolutionised by the likes of IoT, Big Data, and AI, which are all relatively new technology. Financial institutions were the primary beneficiaries of the revolution's requirement for data security and privacy protection for consumers. Customers' distrust of huge organisations has grown after Equifax's 2017 data breach and Facebook's 2021 data dumps. As part of US federal legislation, financial institutions were required to comply with the Financial Modernization Act of 1999, often known as the Gramm-Leach-Bliley Act of 1999 (GLBA). All financial institutions in the United States of America, including TI, are governed by FTC criteria based on the GLBA framework. An ANN-based content classification technique based on MLP architecture and n-gram feature descriptors is presented in this paper in order to detect and protect sensitive customer information of a well-known Texas Instruments company while safeguarding one of its digital image-document storage systems. The suggested method is compared to other current techniques. Prediction accuracy metrics based on data samples collected from the company's digital document

storage have been determined to be much improved and within the permitted range specified by the company's information security monitoring team.[10]

Patil, S.,ET AL [2021] Despite the fact that popular social media platforms like Twitter, Instagram, and Facebook have become indispensable in our day-to-day lives, each has its own set of pros and cons. Fake news and erroneous information are often disseminated on these platforms, and there is an increasing need for classification and categorization. A new approach for identifying bogus news that integrates machine learning has been developed as a consequence. According to this study, a TF-IDF Vectorizer has been developed that may be used to distinguish between real and fake news. Datasets from Kaggle are used in the implementation. According to the findings, this strategy is successful.[11]

Guha, A.,ET AL [2021] In the last twenty-five to thirty years, the Internet has fundamentally altered almost every business paradigm in existence. Data digitization and management has been revolutionised by the likes of IoT, Big Data, and AI, which are all relatively new technology. Financial institutions were the primary beneficiaries of the revolution's requirement for data security and privacy protection for consumers. Customers' distrust of huge organisations has grown after Equifax's 2017 data breach and Facebook's 2021 data dumps. As part of US federal legislation, financial institutions were required to comply with the Financial Modernization Act of 1999, often known as the Gramm-Leach-Bliley Act of 1999 (GLBA). All financial institutions in the United States of America, including TI, are governed by FTC criteria based on the GLBA framework. An ANN-based content classification technique based on MLP architecture and n-gram feature descriptors is presented in this paper in order to detect and protect sensitive customer information of a well-known Texas Instruments company while safeguarding one of its digital image-document storage systems. The suggested method is compared to other current techniques. Prediction accuracy metrics based on data samples collected from the company's digital document storage have been determined to be much improved and within the permitted range specified by the company's information security monitoring team.[12]

3. Existing System

The mission transporter's ability to support multiple catchphrase requests and provide a last item likeness rating in order to satisfy the earth-shattering records retrieval demand is enormous given the large number of substances consumers and reports in the IoT. To isolate the outcomes of an experience, the open encryption uses Boolean watchword search or single catchphrase search.

Burden

Single-catchphrase look without situating

Boolean-watchword look for without situating

Single-watchword look for with situating

4. Proposed System

When we format and cure the outrageous security problem of mixed IoT pieces of knowledge (MRSE), we put up a set of demanding privatives necessities that will make a pleasant IoT information usage device a reality. "Encourage organization" is an effective rule among the many multi-catchphrase semantics.

4.1 Proposed Scheme

At this point, we provide a complete picture of our plan. An inactive semantic multi-catchphrase located search may be set into action by renting "Inert Semantic appraisal."

A. Our Scheme

If the data owner wants to redistribute the mixed-structured data to the IoT server and still have the ability to search for solutions, they must re-proper m records D d 1, d 2, etc., dm. For this, the information owner driver creates a list of secure and accessible key articulations W=extracted from the record collection D, which may be accessed at any time. The reality owner creates a term-report cross section A in accordance with the aforementioned definition of LSA. Lattices A, B, and C may all be deteriorated into the cross section A. After that, we reduce the size of the reliable framework A to produce a new grid A that is determined by the option "reduced size" gauge to the actual term-record organise. One twofold vector Q is given with t key articulations of eagerness for W =as entry.

The MED dataset is used to demonstrate the proposed system's performance in an escalating test assessment. On a PC with a 2.83GHz processor and Windows 7, the whole exam is based on C++ language techniques. Estimates will be reduced to a more manageable level in accordance with the suggested structure. Our system's performance is being evaluated using an extraordinary MRSE plot.

B. Proficiency

It's everything laid out here except for one thing: the KeyGen calculation. We use Gauss-Jordan to enrol the other system in our arrangement. The fraction of the network determines when to create keys. As a result, the SVD set of standards offered by SVD arrangement will take up a lot of time. There are many different calculations, a wide range of rundown production and trapdoor advancement to support the amazing MRSE that is offered via us.

C. Measure

Regardless of all that, in this study, we employ the full scope of usual data recovery. We may initially present the liveliness of accuracy and audit before introducing the F-notion. degree's Recover is the division of significant models that can be recovered, while precision is the portion of recovered instances that may be suitable. Precision and auditing are both based on data and a relevant dimension. The concordant prescribe of precision and recall is an F-measure that combines precision and survey. Legitimately, we use the F-degree to gauge the final outcome of our experiments.

Proposed Algorithm

Algorithm: 1 GenP artitions*(W, τ)*

Input: "W, the Keyword Dictionary."

Output: Partition List (P L) of Keywords.

Step 1: Initialize P L =∅;

Step 2: In the case when W is a keyword partition, add W to P L;

Step 3: **While** | PL | < τ **do**

Step 4: P_{max} = *max(PL);*

Step 5: Use the Normalized Google-Distance of keywords in a bisecting k-means clustering method on the partition Pmax, and then add the resulting two keyword clusters to partition P L;

Step 6: **End** while

Step 7: **Return** PL

5. Result Analysis

Our suggested arrangement outperforms the considerable MRSE in F-measure for a perfect multidimensional nature. Due to its unusual arrangement, it must neglect various similar articulations that are closely related to the watchwords. Regardless, our approach may compensate for this shortcoming and obtain the most important related information. Fig.2 shows that our technique yields a first-rate outcome. Number of reports in this dataset: 50 one hundred fifty-two hundred 0.0.4 0.0.6 0.0.7 LSA-MRSE MRSE-Specific Array.

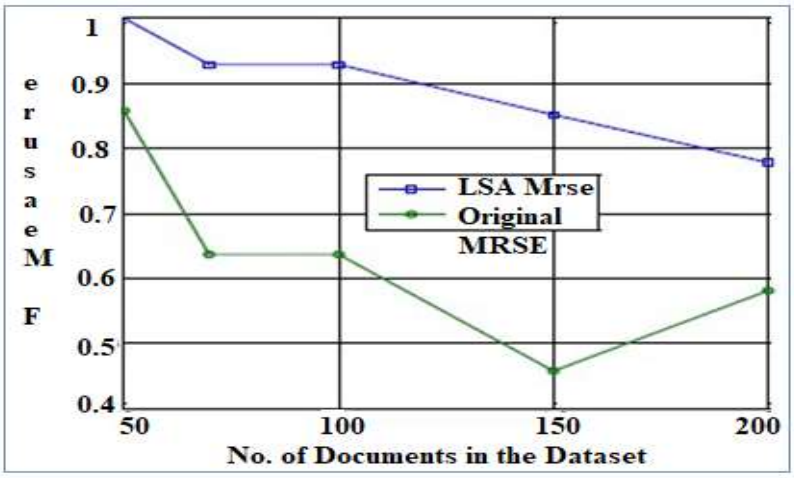

Figure.2. Comparison of two schemes

Differences between a differentiated and standard vector space become more apparent as the torpid semantic spaces become smaller. Whatever the case may be, it's impossible to get a better final product from a lower estimate again. The test and shrinking of individual dimensions, for example, may be done using 100 MED archives. Figure 3 depicts a twist in the recall metric. When can be seen in Figure3, as the number of participants drops from 100 to 30, there is no longer any need for a review. It's almost time to get back the important records. Naturally, the survey's estimates decrease when the number of participants decreases from the initial 30. It means that crucial records cannot be accessed. As a result, when conducting the tests, we must choose the appropriate sample size in order to get the best preliminary results.

0 20 40 60 eighty 100 0.2 zero.3 zero.4 zero.5 0.6 zero.7 0. Eight zero.91 Measurements consider

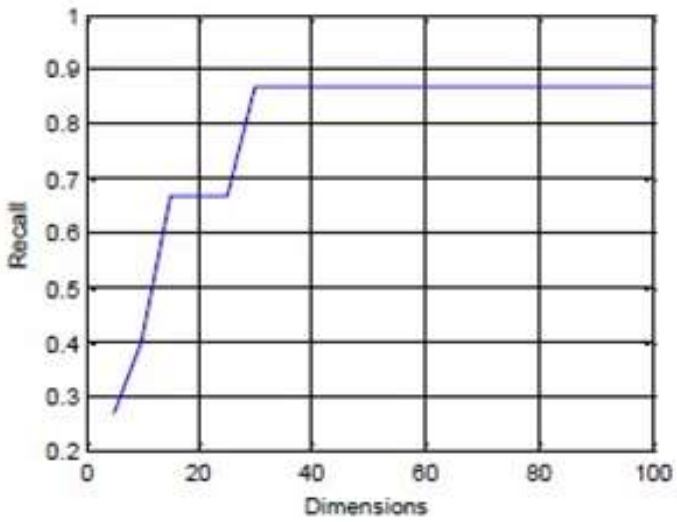

Figure.3. Recall of separate dimensions

Security Analysis:

It is based on the specified security requirements in design dreams: worldwide magazine of security and its bundles that we analyse our recommended strategy

1) Confidentiality of the Index. Due to the jumbled nature of the data in our proposed system, the IoT server is unable to decode the main facts vector from the request vector without the secret key SK. Devaluations can't be inferred from result significance ratings on the IoT server, as stated in. Additionally, the record mystery is a part of this package In the second place, T.

2) the Trapdoor Unlink feature. As a result of the subjective job, a similar search for sales is transformed into distinct request trapdoors. In addition, if necessary, the investigation unlink ability is protected in specific.

3) Privatives are a crucial term in this section. The IoT server should contain additional information, near to the course TF calculations of catchphrases in the dataset, if the backdrop scheme is included. The IoT server is ready to look at these particular distributions and is familiar with the catchphrases that are associated with them. While there is only one query keyword, the TF distributions of important articulations may be immediately spewed out. This means that TF distributions of important articulations with the phonetic properties will be difficult to decipher from our suggested arrangement.

The tagline "Security" has been secured.

6. Conclusion

This work proposes a search strategy based on several watchwords that searches encoded IoT data and then supports a sluggish semantic search. To generate reports, we make use of vectors that combine TF value records. It is from this lattice that we examine the latent semantic relationship between articulations and archives using LSA approaches. In order to obtain the privilege-positioned outcomes and protect the conviction of the experiences, we use an acceptable splitting KNN algorithm to encrypt the list and the addressed vector. If implemented, it would be possible to provide information about not just the exact matching files, but maybe also information about any articulations that could be loosely semantically related with the query term. Future work can be done to guarantee that we can deal with the more advanced semantic catchphrase search for.

References

[1] Jaikar, A., & Noh, S. Y. (2017, May). NOVEL: NO-VowEL Technique to Search Fuzzy Keyword. In 2017 18th IEEE International Conference on Mobile Data Management (MDM) (pp. 315-319). IEEE.

[2] Fan, K., Yin, J., Wang, J., Li, H., & Yang, Y. (2017, December). Multi-keyword fuzzy and sortable ciphertext retrieval scheme for big data. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.

[3] Wang, H., He, J., Zhang, X., & Liu, S. (2020). A short text classification method based on N-gram and CNN. Chinese Journal of Electronics, 29(2), 248-254.

[4] Kaur, S., Sikka, G., & Awasthi, L. K. (2018, December). Sentiment Analysis Approach Based on N-gram and KNN Classifier. In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 1-4). IEEE.

[5] Violos, J., Tserpes, K., Varlamis, I., & Varvarigou, T. (2018). Text classification using the n-gram graph representation model over high frequency data streams. Frontiers in Applied Mathematics and Statistics, 4, 41.

[6] Ali, M., Shiaeles, S., Bendiab, G., & Ghita, B. (2020). MALGRA: Machine learning and N-gram malware feature extraction and detection system. Electronics, 9(11), 1777.

[7] Peng, J., Choo, K. K. R., & Ashman, H. (2016). Bit-level n-gram based forensic authorship analysis on social media: Identifying individuals from linguistic profiles. Journal of Network and Computer Applications, 70, 171-182.

[8] Chen, J., He, K., Deng, L., Yuan, Q., Du, R., Xiang, Y., & Wu, J. (2017). EliMFS: achieving efficient, leakage-resilient, and multi-keyword fuzzy search on encrypted IoT data. IEEE Transactions on Services Computing, 13(6), 1072-1085.

[9] Liu, D., Zhang, X., Feng, Y., & Jones, J. A. (2018, March). Generating descriptions for screenshots to assist crowdsourced testing. In 2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 492-496). IEEE.

[10] Guha, A., Samanta, D., Banerjee, A., & Agarwal, D. (2021). A deep learning model for information loss prevention from multi-page digital documents. IEEE Access, 9, 80451-80465.

[11] Patil, S., Vairagade, S., & Theng, D. (2021, November). Machine learning techniques for the classification of fake news. In 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA) (pp. 1-5). IEEE.

[12] Guha, A., Samanta, D., Banerjee, A., & Agarwal, D. (2021). A deep learning model for information loss prevention from multi-page digital documents. IEEE Access, 9, 80451-80465.

[13] Saikumar, K., & Rajesh, V. (2020). A novel implementation heart diagnosis system based on random forest machine learning technique. International Journal of Pharmaceutical Research, 12, 3904-3916.

[14] Raju, K., Chinna Rao, B., Saikumar, K., & Lakshman Pratap, N. (2022). An Optimal Hybrid Solution to Local and Global Facial Recognition Through Machine Learning. In A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems (pp. 203-226). Springer, Cham.

[15] Sankara Babu, B., Nalajala, S., Sarada, K., Muniraju Naidu, V., Yamsani, N., & Saikumar, K. (2022). Machine Learning Based Online Handwritten Telugu Letters Recognition for Different Domains. In A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems (pp. 227-241). Springer, Cham.

Biography of corresponding author-1

Mr. J N S S Janardhan Naidu currently working as Assistant Professor in the Department of Computer Science and Engineering at Engineering at Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh – 534202. I am having more than 13 years of academic experience. He received B.Tech (IT) in 2004, and M.Tech (IT) in 2007. His area of interests includes Big Data, Cloud Computing, IoT and Blockchain Technology.

Biography of corresponding author-2

Dr. E.N.Ganesh did my doctorate and post doctorate fellowship in the field of Nanotechnology and Post graduate M.Tech in Microelectronics from IIT Madras. I am having 24 years of Teaching Experience and 12 years served as Principal in leading Engineering colleges in Chennai. My PhD Thesis selected as Best thesis and awarded gold medalist. I have published four patents and two Copyrights in the field of biomedical engineering. 6 research projects completed from Government of India and at Present 1 crore projects on 5g related to tamilnadu fisherman problem is in progress. To my credit I have 270 Journal publications and 50 Conference Publications in the area of Nanoelctronics, Bio Medical Engineering. 14 awards from National and International are my credits in the area from Teaching, research and administration. I wrote 8 books for both national and International Publishers. With two decades of admission and administrative experience in engineering colleges in and around Chennai, I am ready to discuss with you regarding admission and other matters in this forum. At Present I am working as Dean School of Engineering VISTAS, VELS University Pallavaram Chennai.