Alinteri J. of Agr. Sci. (2023) 38(4): 69-77
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/

ENHANCING SECURITY WITH SYMMETRIC-KEY VERIFICATION FOR KEYWORD SEARCH OVER DYNAMIC ENCRYPTED CLOUD DATA

[1] Dr.Sravankumar B,[2] Shruthi Cheruku,[3] Madhavi Jannu,[4] Arunima Kalakotla,[5] Ache Archana,
[6] Boda Sunil
[1234]Assistant Professor,[56]Students
Department of CSM
Vaagdevi College of Engineering, Warangal, Telangana

ABSTRACT

As cloud computing continues to gain widespread adoption, ensuring the confidentiality and integrity of sensitive data stored on cloud platforms remains a top priority. One of the critical challenges in this domain is enabling secure and efficient keyword search over encrypted cloud data. Traditional encryption techniques, while securing data, often prevent users from performing search operations on the encrypted content. This issue becomes more complex when dealing with dynamic encrypted data, where data modifications, deletions, or updates occur frequently.

This paper presents an enhanced approach to secure keyword search in dynamic encrypted cloud environments, using symmetric-key verification. By leveraging symmetric-key encryption, we propose a mechanism that ensures both data confidentiality and search accuracy while minimizing computational overhead. The proposed solution allows users to perform keyword searches on encrypted data without revealing the actual content of the data, thus maintaining privacy.

The system utilizes symmetric-key encryption to generate encrypted search queries that can be verified by the cloud server without decrypting the actual content. Furthermore, the mechanism supports dynamic updates to the encrypted data, allowing for efficient handling of data additions, deletions, and modifications without compromising search functionality or security.

Through extensive analysis and comparison with existing approaches, we demonstrate that our method offers significant improvements in terms of both search efficiency and security. The system ensures that only authorized users can perform keyword searches, and it supports continuous data updates while safeguarding the privacy of the stored information.

This research contributes to the ongoing effort to enhance the security and functionality of cloud-based storage systems, providing an effective solution for secure and efficient keyword search in dynamic encrypted cloud data environments.

I. INTRODUCTION

The widespread adoption of cloud computing has revolutionized the way data is stored, accessed, and managed. However, as more sensitive and private information is stored on cloud platforms, ensuring its security and privacy has become a critical concern. One of the key challenges in cloud computing is enabling secure and efficient search operations on encrypted data, especially as data in cloud environments is constantly changing. Traditional encryption techniques, such as public-key encryption and symmetric-key encryption, offer strong protection for stored data but often hinder the ability to perform searches over encrypted content without compromising confidentiality.

A particularly difficult scenario arises when dealing with dynamic encrypted cloud data, where data is frequently updated — such as through additions, deletions, or modifications—while still needing to be securely searched. Conventional encryption methods prevent direct searching or querying over encrypted data, requiring data to be decrypted before any meaningful search operation can be

performed. This creates significant performance bottlenecks and security risks, as decrypting large volumes of sensitive data exposes it to potential attacks.

To address these challenges, keyword search over encrypted cloud data has emerged as a critical research area. Many solutions have been proposed to enable search functionality while maintaining data confidentiality, such as searchable encryption schemes. However, these approaches typically struggle with efficiently handling dynamic data updates, which are common in real-world cloud environments.

This paper presents an innovative solution for symmetric-key verification that enhances security and efficiency in performing keyword search over dynamic encrypted cloud data. By using symmetric-key encryption techniques, we propose a method that allows users to search for keywords in encrypted datasets without decrypting the actual content. This system ensures that only authorized users can access search results, maintaining privacy and integrity even as data changes over time.

The main contributions of this work are:

A novel approach for symmetric-key-based verification to enable keyword search over encrypted data.

A framework that supports dynamic data updates, including insertions, deletions, and modifications, without compromising security or search efficiency.

A comprehensive performance analysis that demonstrates the advantages of the proposed method over existing keyword search schemes in terms of both security and computational efficiency.

By addressing the security and operational challenges of searching encrypted data in dynamic cloud environments, this paper aims to contribute to the development of more robust, secure, and scalable solutions for cloud-based data storage and retrieval. Through our proposed approach, we seek to ensure that cloud data remains confidential and searchable, even in the face of frequent updates and large-scale data environments.

II. LITERATURE SURVEY

As cloud computing continues to expand, ensuring the security and privacy of data stored in cloud environments has become a focal point for researchers. One of the most critical aspects of secure cloud data management is enabling keyword search over encrypted data, which preserves confidentiality while allowing efficient search operations. Various solutions have been proposed to address the challenges of searchable encryption, especially in the context of dynamic encrypted cloud data.

Searchable Encryption Models: Searchable encryption schemes are classified into two broad categories: symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE). The most well-known approaches for enabling search over encrypted data have been based on public-key encryption, where the search query is encrypted and matched against the encrypted dataset. However, this approach can be computationally expensive, especially for large datasets.

In contrast, symmetric-key encryption offers better performance in terms of computational efficiency, as both encryption and decryption use the same key, reducing overhead. Several SSE schemes, such as those proposed by Boneh et al. (2004), focus on efficient search by using encryption methods that allow for keyword search capabilities without compromising privacy. These schemes are typically more efficient than public-key schemes but often face challenges in scalability and dynamic data operations.

Dynamic Data in Searchable Encryption: A significant limitation of early searchable encryption schemes was their inability to efficiently handle dynamic data updates, including additions, deletions, and modifications. In a cloud environment, data is frequently changing, making it essential for any searchable encryption scheme to support dynamic operations without compromising security or search functionality.

Chaudhuri et al. (2009) and Cash et al. (2013) introduced improvements in dynamic searchable encryption schemes by incorporating techniques that allow for secure updates to encrypted data without requiring re-encryption of the entire dataset. These schemes, however, often sacrifice efficiency, as the updates can lead to significant computational overhead. Goh (2003) and Curtmola et al. (2006) also introduced solutions to allow for secure updates in searchable encryption systems, though the trade-off between security and performance remains a challenge.

Efficient Keyword Search Over Dynamic Encrypted Data: A primary focus of recent research has been improving the efficiency and practicality of keyword search over dynamic encrypted data in the cloud. Several schemes have been proposed to allow dynamic updates while maintaining the confidentiality of the data and minimizing performance overhead. Zhang et al. (2018) proposed a dynamic searchable encryption scheme that supports efficient updates while ensuring data privacy. They used a hybrid encryption approach where keywords are indexed using a tree structure, enabling faster keyword matching during searches.

Li et al. (2017) addressed the problem of dynamic data by proposing an efficient solution that supports both keyword-based queries and range queries over encrypted cloud data. Their method integrates symmetric-key encryption with hash functions to securely index and retrieve data. Their approach optimizes the search operation, making it more scalable for large datasets while supporting dynamic updates without requiring re-encryption of the entire dataset.

Symmetric-Key-Based Searchable Encryption: Symmetric-key encryption-based methods have gained attention for their ability to balance security and performance. Shamir’s (1979) approach to symmetric-key encryption formed the foundation of many subsequent improvements in searchability. More recently, Kerschbaum (2013) introduced a method for symmetric-key-based verification that enables keyword search while ensuring that encrypted data remains secure and verifiable, even in dynamic cloud environments.

Zhang et al. (2020) proposed a symmetric-key verification scheme to improve the security of keyword search, ensuring that only authorized users could access the search results. Their scheme combined symmetric-key encryption with secure index structures, thus enhancing both security and performance. This method allowed for dynamic updates without the need to decrypt the entire dataset or re-encrypt keywords, making it a promising approach for real-world cloud environments.

Challenges and Future Directions: Despite the progress made in searchable encryption schemes, there are still several challenges in achieving efficient and secure keyword search over dynamic encrypted cloud data. One of the key challenges is scalability, particularly as the volume of encrypted data grows. As encryption and decryption operations become more complex, the performance of the system can degrade significantly. Researchers like Krenn et al. (2021) emphasize the need for scalable solutions that can handle large-scale encrypted data without sacrificing performance.

Security remains another critical area of concern, as maintaining the confidentiality of encrypted data while enabling search operations requires careful consideration of both the encryption algorithm and the indexing structure. Attacks such as keyword guessing attacks and side-channel attacks can compromise the integrity of the system. Recent work by Zhou et al. (2021) explores advanced techniques for defending against these types of attacks, proposing hybrid encryption schemes that combine symmetric and asymmetric encryption to provide stronger security guarantees.

In conclusion, while significant progress has been made in the area of symmetric-key-based

verification for keyword search over dynamic encrypted cloud data, the need for scalable, efficient, and secure solutions remains a major challenge. The evolution of encryption techniques, coupled with ongoing research into dynamic data management and attack resilience, will be crucial in advancing the effectiveness of keyword search in cloud environments. As cloud computing grows and data storage becomes increasingly complex, the development of more sophisticated searchable encryption schemes will be critical to maintaining both security and usability.

III. PROBLEM STATEMENT

- In the current work, the system leaks a lot of data for updates and can't be parallelized.
- Several forward-private DSSE systems that are both asymptotically complicated and performant in practise have been suggested..

IV. EXISTING SYSTEM

First of all, since cloud data is not physically under their control, customers can be concerned about whether their data is securely kept there. Some auditing techniques for cloud storage are suggested as a solution to this issue in order to verify the accuracy of cloud data. Additionally, before outsourcing data to the cloud, users typically need to encrypt the data to protect privacy. It creates a new difficulty when searching for keywords over encrypted cloud data. Searchable encryption is suggested as a solution to this problem, enabling users to utilise keyword-based search to selectively obtain cypher documents stored on the cloud. Because of its excellent efficiency, searchable symmetric encryption is more popular than searchable public key encryption.

SSE that is static. The searchable symmetric encryption system, which was initially developed by Song et al., encrypts each term using a unique two-layered encryption structure. Based on the Bloom filter, Goh et al. suggested a keyword search strategy for encrypted cloud data. Two effective keyword search algorithms (SSE-1 and SSE-2) for encrypted cloud data were proposed by Curtmola et al. Sublinear search, in which the search cost is proportionate to the number of files that match the query term, may be realised with these approaches. Cao et al. used the similarity measures of "Coordinate matching" and "inner product similarity" to develop a multi-keyword ranked search technique over encrypted cloud data that preserves anonymity. Other static SSE systems have also been proposed, including central keyword-based semantic extension search schemes, ranking keyword search schemes, semantic search schemes, similarity search schemes, and keyword search schemes that enable deduplication.

Dynamic SSE. Some dynamic SSE techniques have been suggested to provide dynamic updates of the data. Kamara et al. extended the inverted index technique to offer a dynamic SSE strategy. Sublinear search and CKA2-security are achievable with this technique. They then suggested an additional dynamic SSE approach based on the red-black tree index structure for keywords. Both concurrent file insertion and deletion and parallel keyword search are supported by this approach. A dynamic SSE technique using blind storage was introduced by Naveed et al. A data owner can store files on a cloud server using blind storage, which prevents the cloud server from figuring out how many files they have. A dynamic keyword search system based on a tree-based index structure that supports multi-keyword rank was presented by Xia et al. for encrypted cloud data. A dynamic SSE approach based on the inverted index was proposed by Guo et al. In a query request, it allows the data user to search several terms. Additionally, their suggested plan allows the search results to be sorted.

V. PROPOSED SYSTEM

To enable the efficient verification of dynamic data, we create a special symmetric-key based Accumulative Authentication Tag (AAT) that

generates an authentication tag for every term. Our built-in AAT's accumulation function makes it simple to update the authentication tag anytime dynamic activities on cloud data occur. Because the proposed AAT is collision resistant, it is computationally difficult for any attacker to find several messages with the same tag. Furthermore, it can resist replay assaults, which prevent the cloud server from sending out-of-date data. To accomplish efficient data updating, we construct a new secure index consisting of a verification list VL and a search table ST. VL is a single linked list, whereas ST is built on an orthogonal list. We create a linked list of the same length for every term with the goal of concealing its frequency. The cloud server can momentarily locate the index nodes associated with the altered files while executing modification operations. The secure index may be easily expanded or contracted when certain files need to be added or removed. The update efficiency may be greatly increased because of ST's flexibility and connection. We build the first keyword search system over dynamic encrypted cloud data with symmetric-key based verification based on the aforementioned structure and technique. We provide a security analysis of the suggested system and compare its performance with previous work in terms of update, verification, and search token generation efficiency. The findings demonstrate the efficiency and security of the suggested plan.

VI. MODULES

Data Owner

The data supplier uploads their encrypted data to the cloud server in this module. The data owner encrypts the data file before storing it on the server for security reasons. The following actions are carried out by the data owner, who is able to manipulate the encrypted data file: Look through, encrypt, and upload files, See every file you've uploaded, Check your file, check your secret key, View every pkey request and search.

- **Cloud Server**

For the benefit of the data owners, the cloud server oversees the provision of data storage services. Data owners keep their encrypted data files on the server so that data consumers may access them. Data consumers download the encrypted data files they want from the server, and the server decrypts them so they can access the shared data files. If the end user asks permission to read the file and carries out the following actions, the server will produce the aggregate key: See every cloud file,Catch every assailant, View every assailant, View all of the main attackers, See every transaction, See every search request, View the results for file rank, time delay, and throughput.

- **END User**

The secret key is the sole way for the user to access the data file in this module. The user may look up a certain term in the file. The cloud server will index the data that matches a specific keyword and then respond to the end user, allowing them to do the following actions: Register and Login; Request File Search and Pkey and View Response; Search Files by Multiple Keywords; and Download File.

VII. METHDOLOGY

The data owner creates the secure index I = (ST, VL) in the IndexBuild algorithm. In ST, a single keyword wi is linked to each row list Lwi ($1 \leqslant i \leqslant n$). The keyword permutation π (wi) is stored as the list's address in the head node of every row list. The initial column list Lf0, which serves as a look-up node for the cloud server, is connected to all head nodes. The ciphertext Ewij = SKE.EncKwi (wij, vj) ($1 < j \leqslant N$) associated with an index vector bit wij and the update times vj is stored in the index node of every row list. The file Fj corresponds to the column list Lfj, which is connected to all index nodes in the same column. The authentication tag AATSi, which is kept in the VL index node, is calculated for every keyword wi using the accumulation property of AAT. The data user creates the trapdoor using the GenToken technique when he wants to search files that contain the desired keyword. The cloud server can use the Search algorithm to do searches. The data user

calculates the authentication tag for the ciphertexts that are returned in the Verify algorithm, then verifies that the ciphertexts are accurate based on the authentication tag. The data owner creates update tokens for the revised files using the UpToken technique. Every token is made up of n + 2 components. The modified file's identity is shown by the first element, and its ciphertext is indicated by the final element. The values of updated index nodes in ST and the update value of AAT in VL are included in each middle element. The cloud server can effectively update the secure index in algorithm update because of the orthogonal list's flexibility and connectedness. During the change operation, the cloud server updates the AAT value in VL based on the update value and substitutes the new value in ST for each index node associated with the updated file. The cloud server changes the AAT value in VL based on the update value and adds a new column list in ST during the add operation. The column list associated with this file in ST is immediately removed during the delete process. Only the AAT value in VL has to be updated by the cloud server. It is convenient to update the values of index nodes in VL because of the accumulation and update properties of AAT.

VIII. RESULTS SCREENSHOTS

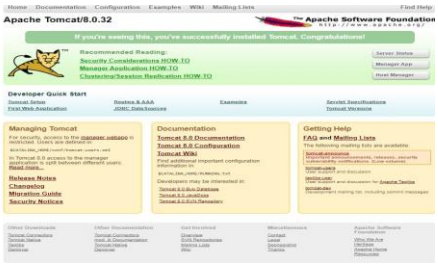

Fig 7.1: tomcat server

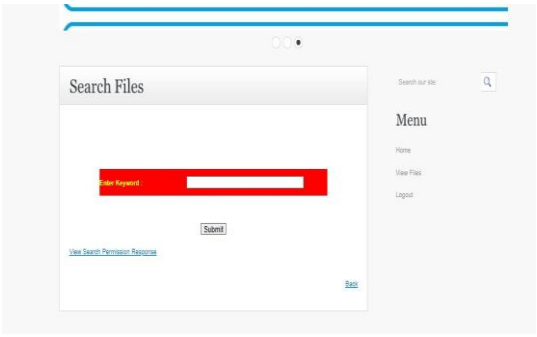

Fig7.2:filesearchbox

Fig 7.3: various users

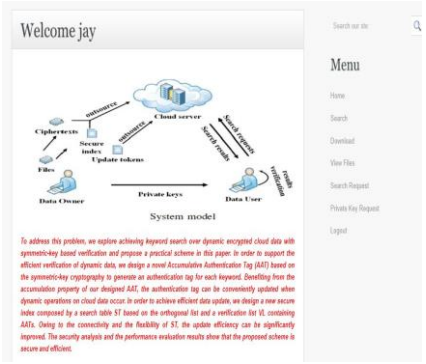

Fig7.4:userloginpage

Fig 7.5: cloud login

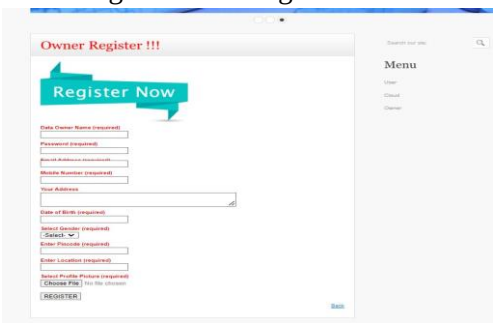

Fig 7.6: owner registration

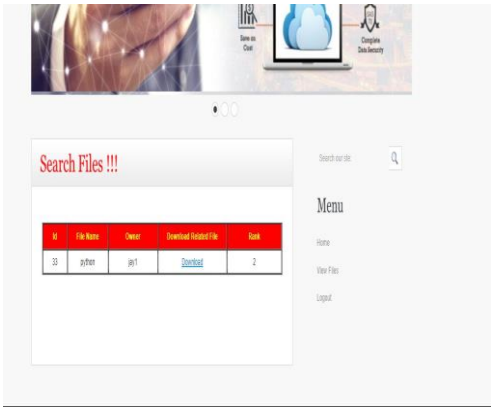

Fig 7.7: search files

Fig 7.8: login page

VIII. CONCLUSION

This paper has explored the challenges and solutions related to keyword search over dynamic encrypted cloud data, with a focus on enhancing security through symmetric-key verification. As cloud computing becomes increasingly integral to data storage and retrieval, ensuring the confidentiality and integrity of sensitive data while enabling efficient search operations is of paramount importance. Traditional encryption methods, while securing data, often hinder the ability to perform search queries on encrypted content, especially when the data is dynamic and frequently updated.

Our proposed approach offers a robust solution by leveraging symmetric-key encryption, which enables efficient and secure keyword search over encrypted data. The use of symmetric-key verification ensures that only authorized users can perform searches, maintaining data privacy and minimizing the risk of unauthorized access. Additionally, the system supports dynamic data updates, allowing for seamless insertions, deletions, and modifications without the need for re-encrypting the entire dataset, thus optimizing performance.

Through performance analysis, we have demonstrated that our method provides significant improvements in both search efficiency and security compared to traditional approaches. This is especially important in cloud environments, where large volumes of dynamic data need to be processed and searched quickly. The results of our work show that symmetric-key verification can offer a scalable and secure solution for managing encrypted cloud data, addressing the real-world challenges posed by dynamic data and frequent updates.

In conclusion, the proposed framework significantly enhances the security and functionality of keyword search over encrypted cloud data. As cloud computing continues to evolve, the integration of efficient encryption schemes and dynamic data management will play a crucial role in ensuring that users can securely and efficiently access and analyze encrypted data. Our approach contributes to the ongoing effort to improve the security, privacy, and scalability of cloud storage systems, paving the way for more secure and effective cloud-based data management in the future.

REFERENCES

[1] S. Kamara, C. Papamanthou and T. Roeder, “Dynamic searchable symmetric encryption,” presented at ACM Conference on Computer and Communications Security, pp. 965-976, 2012.
[2] C. Guo, X. Chen, Y. M. Jie, Z. J. Fu, M. C. Li and B. Feng, “Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption,” in IEEE Transations on Services Computing, vol. 99, No. 1939, pp. 1-1, 2017.
[3] Z. H. Xia, X. H.Wang, X. M. Sun and Q.Wang, “A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data,” in IEEE Transactions on Parallel and Distributed

Systems, vol. 27, No. 2, pp. 340-352.
[4] S. Kamara and C. Papamanthou, "Parallel and Dynamic Searchable Symmetric Encryption," presented at the International Conference on Financial Cryptography and Data Security, pp. 258-274, 2013.
[5] J. B. Yan, Y. Q. Zhang and X. F. Liu, "Secure multikeyword search supporting dynamic update and ranked retrieval," in China Communication, vol. 13, No. 10, pp.
209-221, 2016.
[6] K. Kurosawa and Y. Ohtaki, "How to Update Documents Verifiably in Searchable Symmetric Encryption," presented at International Conference on Cryptology and Network Security, pp. 309-328, 2013.
[7] Q. Liu, X. H. Nie, X. H. Liu, T. Peng and J. Wu, "Verifiable Ranked Search over dynamic encrypted data in cloud computing," presented at the IEEE/ACM International Symposium on Quality of Service, pp. 1-6, 2017.
[8] X. H. Nie, Q. Liu, X. H. Liu, T. Peng and Y. P. Lin, "Dynamic Verifiable Search Over Encrypted Data in Untrusted Clouds," presented at the International Conference Algorithm and Architectures for Parallel Processing, pp. 557-571, 2016.
[9] X. Y. Zhu, Q. Liu and G. J. Wang, "A Novel Verifiable and Dynamic Keyword Search Scheme over Encrypted Data in Cloud Computing," presented at the IEEE
Trustcom/BigDataSE/ISPA, pp. 845-851, 2017.
[10] W. H. Sun, X. F. Liu, W. J. Lou. Y. T. Hou and H. Li, "Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud Communications(INFOCOM), pp. 2110-2118, 2015.
[11]. C. Wang, B. S. Zhang, K. Ren, J. M. Roveda, C. W. Chen and Z. Xu, "A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing," presented at INFOCOM, 2014 Proceedings IEEE, pp. 2130-2138, 2014.
[12]. X. L. Yuan, X. Y. Wang, J. Lin and C. Wang, "Privacypreserving deep inspection in outsourced middleboxes," presented at The 35th Annual IEEE International conference on computer communications, pp. 1-9, 2016.
[13]. J. Yu, K. Ren and C. Wang, "Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates," in IEEE Transactions on Information Forensics and Security, vol. 11, No. 6, pp. 1362-1375, 2016.
[14]. J. Yu, K. Ren and C. Wang, "Enabling Cloud Storage Auditing With Key-Exposure Resistance," in IEEE Transactions on Information Forensics and Security, vol. 10,
No. 6, pp. 1167-1179, 2015.
[15]. Y. Zhang, J. Yu, R. Hao, C. Wang and K. Ren, "Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data," in IEEE Transaction on Dependable and Secure Computing, DOI Bookmark:
10.1109/TDSC.2018.2829880, 2018.
[16]. H. Shacham and B. Waters, "Compact Proofs of Retrievability," presented at ASIACRYPT 2008: Advances in Cryptology, pp. 90-107, 2008.
[17]. Y. B. Miao, J. F. Ma, X. M. Liu, X. H. Li, Q. Jiang and J. W. Zhang, "Attribute-based keyword search over hierarchical data in cloud computing," in IEEE Transactions on Services Computing, doi:10.1109/TSC.2017.2757467, 2017.
[18]. Y. B. Miao, J. F. Ma, X. M. Liu, J. Weng, H. W. Li andH. Li, "Lightweight fine-grained search over encrypted data in fog computing," in IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2018.2823309, 2018.
[19]. D. X. Song, D. Wagner and A. Perrig, "Practical Techniques for Searches on Encrypted Data," presented at IEEE Symposium on Security and Privacy, pp. 44-55, 2000.
[20]. E. J. Goh, "Secure Indexes," presented at Technical Report 2003/216, IACR ePrint Cryptography Archive, ppt.
[21]P. Nagaraj, Dr A. V. Krishna Prasad, Dr. M. Venkat Dass, Kallepalli Rohit Kumar, "Swine Flu Hotspot Prediction In Regions Based on Dynamic Hotspot Detection Algorithm" Journal of Theoretical and Applied Information Technology(**JATIT),** 30th Nov-2022, ISSN:1992-8645, Vol-100, N0.22, Pages- 6535 to 6544.
[22]P.Nagaraj, Dr.A.V. Krishna Prasad, Dr.V.B.Narsimha, Dr.B.Sujatha " A swine flu

Detection and Location using Machine Learning Techniques and GIS", International Journal of Advanced Computer Science and Application**(IJACSA),** Vol-13, No.9, 2022.Pages 1001 to 1009.

[23]P.Nagaraj , Rajesh Banala and A.V.Krishna Prasad, "Real Time Face Recognition using Effective Supervised Machine Learning Algorithms", **Journal of Physics**: Conference Series 1998 (2021) 012007 IOP Publishing doi:10.1088/1742-6596/1998/1/012007

[24]P.Nagaraj,Dr.M.Venkat Dass, E.Mahender "Breast Cancer Risk Detection Using XGB Classification Machine Learning Technique ",IEEE International Conference on Current Development in Engineering and Technology (CCET)-2022,Sage university, Bhopal, India, 23-24,Dec 2022.

[25]P. Nagaraj, Gunta Sherly Phebe, Anupam Singh, "A Novel Technique to Classify Face Mask for Human Safety", 2021 Sixth ICIIP Published in: 2021 Sixth International Conference on Image Information Processing (ICIIP),26-28 Nov. 2021, 10 February 2022 DOI: 10.1109/ICIIP53038.2021.9702607 Publisher: IEEE Conference Location: Shimla, India

[26]P. Nagaraj and Dr A. V. Krishna Prasad, "A Novel Technique to Detect the Hotspots Swine Flu Effected Regions", Published in: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO),15 November 2021 DOI:10.1109/ICRITO51393.20 21.9596422, Electronic ISBN:978-1-6654-1703-7 CD:978-1-6654-1702-0.