Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Anonymous Data Sharing Scheme in Public Cloud and its Application in E-Health Record

Nikhil Sai Reddy Jonnala[1], Manindranath Kalyanapu[2], Dr. Mercy Paul Selvan[3], Dr. Viji Amutha Mary[4], Dr. L. K. Joshila Grace[5] , Dr. S. Jancy[6], Dr. Suji Helen[7]

[1,2] Student, Dept. of CSE, Sathyabama Institute of Science and Technology.

[3,4,5,7] Associate Professor, Dept. of CSE, Sathyabama Institute of Science and Technology.

[6]Assistant Professor, Department of Computer Science, Sathyabama Institute of Science and Technology.

Article Info
Page Number: 1610 – 1621
Publication Issue:
Vol. 71 No. 3s2 (2022)

Article History
Article Received: 22 April 2022
Revised: 10 May 2022
Accepted: 15 June 2022
Publication: 19 July 2022

ABSTRACT
Your health care supplier might be changing from paper records to electronic health records (EHRs) or may as of now be utilizing EHR. EHR permits specialist organizations to utilize data all the more effectively to work on the quality and productivity of your consideration, yetEHR doesn't change the security or security assurances that apply to your wellbeing data. Thistask plans to foster a safe cloud framework for the turn of events and utilization of solid figuringadministrations at all levels of the public cloud plan. This takes out interior and outer security dangers. Accordingly, information protection, data trustworthiness, verification, and approval are accomplished, and dynamic and latent assaults from the cloud network cloud are disposed of. Foster a solid cloud system to get to believed registering and capacity administrations at alllevels of the public cloud utilization model.

Keywords: Attribute-based encryption, cloud computing, data sharing, searchable encryption.

INTRODUCTION

Because of the fast development of data, it is an immense weight on clients to store a ton of data within. Consequently, numerous associations and people need to keep their data in the cloud. Be that as it may, data put away in the cloud can be compromised because of unavoidable programming mistakes, equipment blunders, and human blunder in the cloud. Numerous remote detecting plans are given to guarantee that the data is appropriately put away in the cloud. On account of controller frameworks, the proprietor should initially sign prior to halting the cloud. This mark isutilized during the uprightness check to demonstrate that the cloud contains data. The proprietor then, at that point, places the cloud data in the cloud with the comparing mark. Distributed storage data is shared by numerous clients on many distributed storage applications like Google Drive, Dropbox, and iCloud. Sharing data is perhaps the most widely recognized distributed storage application, permitting numerous clients to impart data to other people. In any case, this common data might be cloud-based. For instance,electronic clinical records put away andpartook in the cloud frequently contain patient classified data, (for example, patientname, phone number, ID number, and so on) and secret data. clinical, (for example, health clinic name). Assuming these EHRsare hung in the cloud for sharing, the secret data of patients and medical clinics will unavoidably be uncovered by the cloud. Likewise, EHR trustworthiness ought to be observed because of

human mistake in the cloud and programming/disappointment. Thusly, it is vital to lead an excellent review to secure the secrecy of shared data. A potential answer for this issue is to duplicate every one of the common records prior to sending them to the cloud, then, at that point, sign a mark that is utilized to confirm the uprightness of the secret document, and afterward glue this secret record with a cloud-related mark. This strategy assists you with concealing secret data, as just the proprietor can download this record. Notwithstanding, this will keep the common record from being totally utilized by others. For instance, identifying the EHR of patients with irresistible sicknesses can secure the protection of patients and clinics, however these shut EHRs may not be very much utilized by analysts. Appropriating the mysterious key to scientists appears to be a potential arrangement. Notwithstanding, it is unimaginable to expect to carry out this technique for the accompanying reasons. To start with, appropriating a mysterious key requires a protected organization, at times hard to give. Moreover, when clients utilize their EHR in the cloud, it tends to be hard to figure out which scientists will utilize their EHR soon. Thus, it is absurd to expect to conceal private data from the capacity to share the whole document. In this way, the most common way of executing the trading of data utilizing secret data under full control of the dad is significant and important. Luckily, this issue didn't show up in past investigations.An undeniable degree of safety is accomplished to give dependable counting and capacity administrations. Know about trustworthiness, secrecy, confirmation and announcing. Obliterate inner and outside security. Stay away from assaults that are basic and direct in nature. Admittance to different degrees of safety in the framework.

RELATED WORK

Securely Outsourcing Attribute-Based Encryption with Checkability. Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang[1].Attribute-Based Encryption (ABE) is a believed cryptographic law that incredibly improves the control framework. Contingent upon the size of the ABE strategy, the size of the primary ABE age and counting is huge. Outside input ABE results can provide someone else with a difficult occupation of computing, however the issue of controlling the responses given by someone else is as yet unsettled. To defeat the previously mentioned impediments, we offer another Secure Outsourced ABE framework that upholds the capacity to identify and open appropriately. Our new methodology records generally sign-in approaches and elements identified with the circumstance of the opening or shutting of Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), leaving just a set number of basic elements.Authority and clients of the option to work in the area. Also, interestingly, we require the development of an ABE to assist us with testing the aftereffects of outside estimations. An extensive security examination is an action that guarantees that the arranged projects are dependable and compelling.

Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter[2].We are investigating the issues of patient medical care in the electronic clinical framework. We accept that security in the framework should be ensured by control just as control frameworks. Moreover, we are discussing how to permit patients to work and store private, secret data about the patient's security while the data community is compromised. The typical contention against this strategy is that encryption

meddles with the working of the framework. In any case, we show that we can make a framework that permits patients to share their privileges, just as quest for their records. We regularly require a patient-focused observing project, every one of which has an alternate cryptographic rule. Cross-Domain Data Sharing in Distributed Electronic Health Record Systems JinyuanSun[3].Interoperability between foundations or organizations that occasionally interface individuals to undeniable level patients is needed by the Electronic Health Record (EHR) framework. A diagram for portrayal ought to be a way for cooperation between organizations, as coordinated effort and sharing and sharing of patient data are viewed as close to home and classified. Step by step instructions to address the freedoms of the accomplice and diminish it. Patients are hesitant to acknowledge the EHR framework except if there is an assurance that their clinical data will be utilized and appropriately conveyed, which can't be effectively accomplished without legitimate line confirmation and checking. Moreover, it is important to suspend the exchange to any even out of collaboration. In this paper, we request a safe EHR framework dependent on cryptographic highlights to adequately share patient data and keep up with patient privacy during cooperation. Our EHR framework incorporates access control systems and suspension prerequisites to refine the essential control and expulsion strategies needed by the strategy utilized. The proposed EHR framework is intended to match the objectives of benefit check between area agents. Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data Ning Cao ; Cong Wang ; Ming Li ; Kui Ren ; Wenjing Lou[4]. Notwithstanding distributed computing, data specialist co- ops are urged to give their own data the executives frameworks, from nearby locales to the overall business cloud, to work with financial investment funds. Notwithstanding, to secure the protection of the media, classified data should be kept secret and customary data dependent on thepursuit catchphrase should be utilized in anobsolete way. Thusly, it is vital to empoweradministration-based protection. Because of the huge number of clients of data and archives in the cloud, it is important to remember undeniable level watchwords forthe inquiry and search necessities, contingent upon where the catchphrases are connected. Catchphrase search activities center around a solitary watchword or Boolean catchphrase, and indexed lists are uncommon. In this article, we will interestingly clarify and resolve the mind- boggling issue of protection, which is the way to tracking down secret data in bookkeeping (MRSE). We give a rundown of pre requisities to a solid cloud working framework. By different key terms, we select the best "interface" connect, i.e., utilize the data booklet however much as could reasonably be expected in the inquiry question. We keep on utilizing "a similar sort of contribution" to assess how much estimation. We initially give an outline of MRSE dependent on inner security items, and afterward an outline of the two best MRSE projects to meet the distinctive explicit necessities of the two dangers. To further develop the website improvement administration experience, we keep on extending the two projects to help more data. Top to bottom examination of individual life and execution ensures. Constant information concentrates on showthat other arranged techniques start at the highest point of figuring and correspondence.

Privacy-Preserving Cloud-Based Personal Health Record System Using Attribute- Based Encryption and Anonymous Multi- Receiver-identity-Based Encryption Changji Wang, Xilei Xu, Dongyuan Shi, Jian Fang[5].As the new norm for patient data trade, cloud-based personal health record (CB-PHR) assumes a significant part in enabling patients and giving

quality clinical consideration. In this article, wehave fostered the book CB-PHR system. Abig part of the believed cloud administrations for PHR holders permit them to keep their wellbeing data private and offer their wellbeing data with numerous PHR clients. To decrease the way to overseeing anything, we diminish the quantity of PHR clients to public security areas and private spaces. PHR holders disguise their general wellbeing data utilizing an encryption-based cryptographic text strategy, while unknown beneficiaries use privacy to conceal their own wellbeing data on the web. Just approved clients with an endorsement that meets the necessities of the scrambled text strategy or their profile is a novel ID that can conceal clinical data. Various dissects and studies have shown that our CB-PHR framework is protected, dependable, adjusted and proficient. CDPS: A cryptographic data publishing system T. Li, Z. Liu, J. Li, C. Jia, K. Li[6]. The customary strategy for distributing data will take out straightforward and multi- reported highlights to accomplish individual security purposes. In a huge media cloud, the prerequisites for the utilization of data (for instance, mining) arenumerous and shifted, which is more than customary techniques. This page gives a data distributing framework that secures the honesty of the data (for instance, the idea of the put away information) and permits you to erase anything and stay unknown without the utilization of invulnerability. Security examination shows that our framework is just about as secure as it ought to be.

Identity-based encryption with outsourced revocation in cloud computing J. Li, J. W. Li, X. Chen, C. Jia, W. Lou[7].Identity- Based Encryption (IBE), which works on the administration of Public Key Infrastructure (PKI) and the public key, is a significant rendition of public knowledge. Notwithstanding, one of the primary impediments of IBE abilities is the expanding number of Private Key Generator (PKG) estimations when utilizing it if there should arise an occurrence of separation. Delayed hardship of conventional PKI is very much considered, however degree the executives is a weight that IBE tries to diminish. In this paper, we require the first re-appropriating computation in the IBE and the IBE program that can be killed utilizing a server to resolve the significant issue of refuting explicit data. Our program directs the greater part of the critical exercises during the vital ages and the way to refreshing the cloud facilitating key, leaving hands down the easiest exercises for PKG and its clients to deal with. This objective is accomplished through another innovation that consolidates joint effort: we utilize a novel mix of every client, we require further advancement that can be affirmed by the most recent Calculation Model. At long last, we present the aftereffects of an enormous scope test to exhibit the presentation of the arranged development server. We use attribute-based encryption (ABE) to distinguish the documents of each PHR patient to give a total, exhaustive command over PHR. As opposed to the past work on dependable product tasks, we zeroed in on various parts of the proprietor, lessening the quantity of clients in the PHR framework in numerous security regions, incredibly decreasing the intricacy of the proprietor and dealing with the clients. Multi-definitive ABE is utilized to permit one to acknowledge the protection of patients simultaneously. Our plan additionally permits you to alter the entrance strategy or record properties, and supports admittance to the client/top elements and breaking the necessary windows as per crisis times. We present various logical and examination things that exhibit the security, size, and capacities of the proposed program. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou[8].Personal health record (PHR) is

another patient-focused method of trading wellbeing data and offering it to others, for example, cloudspecialist co-ops. Nonetheless, it is essential to remember that individual data might be undermined by the servers of other unapproved people. It gives a method for acquiring understanding into PHR prior to delivering it to guarantee that patients control their PHR. Notwithstanding, issues, for example, classification issues, key administration scales, simple access, andhardship of the right clients keep on being difficult for admittance to top caliber, educational data. In this article, we requestanother degree of patient-focused working and a method for checking admittance to data in PHR put away on a confided in A cloud-based approach for interoperable electronic health records (EHRs). A. Bahga, V. Madisetti,[9]. We show a cloud-based way to deal with planning an electronic health record (EHR). Distributed computing gives a lot of individuals who are engaged with ecological wellbeing (patients, specialist co-ops, payers, and so forth) Absence of communication norms and arrangements is a significant hindranceto the trading of wellbeing data between various partners. We give the EHR framework - cloud health information systems technology architecture (CHISTAR) that considers the association utilizing an overall plan strategy utilizing a model that mirrors the universally useful of data and the original of clinical data. property. The parts of the CHISTAR program are constructed utilizing cloud plan, which is comprised of interconnected, contradictory parts. In this article, we will clarify the CHISTAR outline, the intuitive understanding, data reconciliation, and security the executives' techniques.

Designing cloudbased electronic health record system with attribute-based encryption. F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, D. Wong[10]. As bookkeeping developed, electronic health record (EHR) arose as quiet focused consideration, wherepatients decided to store their personal health records (PHRs) on a distant server and offer them with doctors for better treatment. Albeit the new structure has demonstrated to enjoy many benefits at the conventional customer server level, cloud servers can be at various levels relying upon the patient, making patient issues a piece oftheir PHR insider facts. In this paper, we have made a protected, solid, and secure EHR cloud-put together clinical data framework based with respect to cryptography to more readily save and offer PHR and take out patients' interests about PHR protection. be that as it may, not dependable on the server. In light of the fundamental EHR framework, we offer expansions, for example, further developed pursuit and expulsion support, effective facilitating, and overcoming any issues between want to execute. Many reviews are presented in literature by many researchers with respect to ecommerce applications in different domain [11][12][13]. This analysis will surely enable the researchers with the idea of deep learning technique in different applications [14][15][16][17]. Different issues also discussed in machine learning applications [18][19][20].

PROPOSED METHODOLOGY

- Your health services supplier might quit electronic wellbeing records (EHRs) or might be utilizing EHRs.
- EHR permits specialist co-ops toutilize data adequately to work on quality and productivity, however EHR doesn't change your own or security profile dependent on your wellbeing data.

- A venture to foster a protected security framework for the turn of events and utilization of standardprocessing administrations at all degrees of public cloud.
- This eliminates inside and outside security.
- Thus, data protection, media trustworthiness, validation, and copyright are accomplished, and smoothed out and smoothed out exercises from the cloud.
- Develop a dependable framework that can work out and store solid administrations at all degrees of public cloud use.

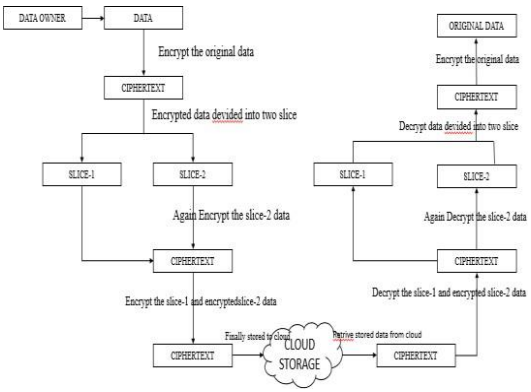

Fig No.1 Proposed Methodology

Advance Encryption Algorithm (AES)

(Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts

data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES Encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

Major advantages of AES over DES are

1. Data block size is 128 bits.
2. Key size 128/192/256 bits depending onversion.
3. Most CPUs now include hardware AESsupport making it very fast.
4. It uses substitution and permutations.
5. Possible keys are 2128, 2192 and 2256[10]
6. More secure than DES.
7. Most adopted symmetric encryptionalgorithm.

Data Encryption Standard (DES)

This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which madeit an insecure block cipher.

Algorithm:

function DES_Encrypt (M, K)where M = (L, R)
M□IP (M)
For round□1 to 16 doK□SK (K, round) L□L xor F(R,Ki)swap(L, R)end
swap (L, R)
M□IP-1 (M)
return MEnd

SHA Algorithm

Step 1: Append Padding Bits….
Message is "padded" with a 1 and as many0's as necessary to bring the message lengthto 64 bits fewer than an even multiple of 512.
Step 2: Append Length....
64 bits are appended to the end of the padded message. These bits hold the binaryformat of 64 bits indicating the length of theoriginal message.
Step 3: Prepare Processing Functions….
SHA1 requires 80 processing functions defined as:
f(t;B,C,D) = (B AND C) OR ((NOT B)AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <=39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <=79)
Step 4: Prepare Processing Constants....
SHA1 requires 80 processing constantwords defined as:
K(t) = 0x5A827999 (0 <= t <= 19)K(t) = 0x6ED9EBA1(20 <= t <=39)K(t) = 0x8F1BBCDC (40 <= t<=59)
K(t) = 0xCA62C1D6(60 <= t <=79)
Step 5: Initialize Buffers….
SHA1 requires 160 bits or 5 buffers ofwords (32 bits):
H0 = 0x67452301 H1 = 0xEFCDAB89 H2 = 0x98BADCFE H3 = 0x10325476 H4 = 0xC3D2E1F0
Step 6: Processing Message in 512-bitblocks (L blocks in total message)
This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.
Input and predefined functions:
M[1, 2, ..., L]: Blocks of the padded andappended message f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing
Functions K(0), K(1), ..., K(79): 80
Processing Constant Words
H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values

- Login/ Registration
- Creation Storage andInstance
- Data Protection
- Data Recovery Module

These are the initial steps to open when a client opens a site. All together for the client to get to the site, the client should enter thesecret word entered during the enlistment cycle. Assuming

the data given by the clientmatches the data in the document, the message expresses that the client hasneglected to get to the site, and the client must reappear the right data. The connect tothe enlistment interaction likewise incorporates the enrollment of new clients.

New clients who need to sign in to the site should enlist before they can sign in. Tapping the Register button to enter will open the enrollment interaction. The new client will enroll by entering theirusername, secret phrase and contact number. The client should return the secret phrase in the text field to affirm the secret word. At the point when the client enters thedata in all text boxes, click the registerbutton to move the data to the data set and afterward the client will return. An enlisted client should be signed in to get to the site. Checks are made in all crates to make the site page work appropriately. Just as the data that ought to be in each composed box, your name, address, secret word, and secret key will be clear at the hour of enlistment. Assuming such an archive is unfilled, the application will give the necessary data to each container. Legitimate enrollment, private data and classified data should be joined. Another affirmation is that the contact number should be 10 digits. On theoff chance that the check is surpassed, the enlistment falls flat and the client must re- register. The message shows up on the site when one of the fields is unfilled. In the event that this data is right, the client will be coordinated to the login page to get to thesite.

CREATING STORAGE ANDINSTANCE

The proprietor can't handle the data in the wake of placing it in the cloud. In thismodule, the first data is put away in two distinct ways. Information for each part canbe observed utilizing diverse open calculations and mystery keys prior to being put away in the Cloud.

DATA PROTECTION

The method of this module is to store information securely and dependably to forestall information access and information section, which will diminish the expense and season of putting awaysecret data in the Cloud storehouse.

DATA RECOVERY

The client can recuperate thedata from the server utilizing various kindsof techniques.

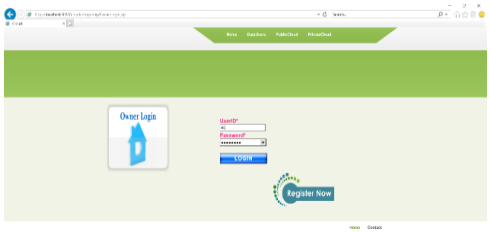

Fig No.3 Login Page

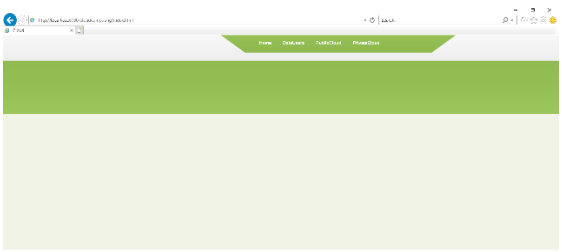

Fig No.2 Home Page

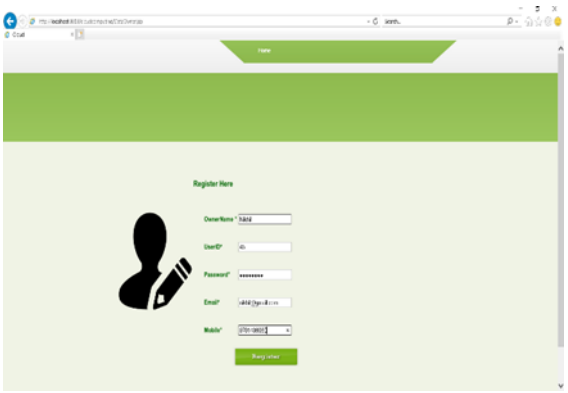

Fig No.4 Registration Page

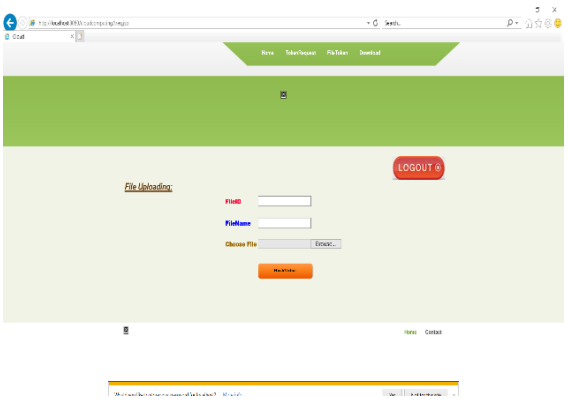

Fig No.5 File Upload Page

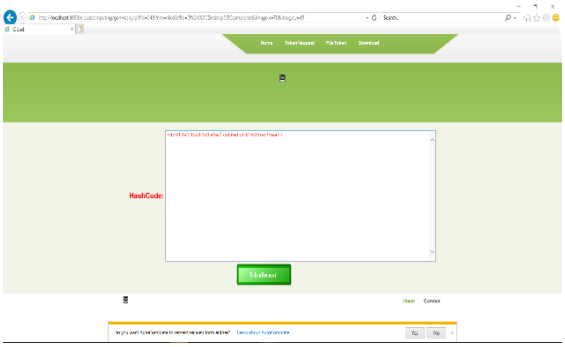

Fig No.6 Token Request Page

Fig No.7 Private Cloud

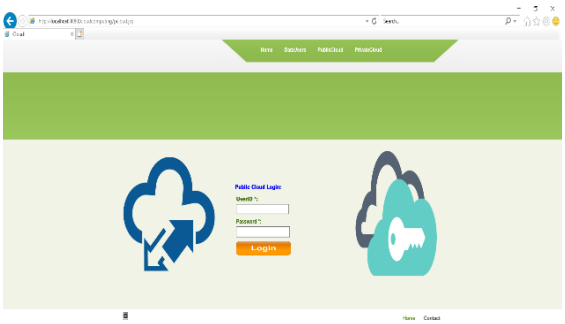

Fig No.8 Public Cloud

CONCLUSION

In this article, we need an arrangement to share data that could prompt obscurity and privacy in the public cloud. We get ready data and security models. We then, at that point, set up a down to earth data trade program and gave a security declaration. The security examination uncovered our security plan true to form. Execution examination shows that our program is being carried out.

REFERENCES

1. C. Chu, S. Chow, W. Tzeng, J. Zhou, R.Deng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, Feb. 2014.
2. Y. Tong, J. Sun, S. Chow, P. Li, “Cloud-assisted mobile-access of health data with privacy and auditability”, IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, Mar. 2014.
3. Z. Pervez, A. Khattak, S. Lee, Y. Lee, “SAPDS: Self-healing attributebased privacy aware data sharing in cloud”, The Journal of Supercomputing, vol. 62, no. 1, pp. 431´lC460, Oct. 2012.
4. Pepsi M, B. B. ., V. . S, and A. . A. “Tree Based Boosting Algorithm to Tackle the Overfitting in Healthcare Data”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 41-47, doi:10.17762/ijritcc.v10i5.5552.
5. C. Fan, V. Huang, H. Rung, “Arbitrary- state attribute-based encryption with dynamic membership”, IEEE Transactions on Computers, vol. 63, no. 8, pp. 1951- 1961, Apr. 2013.
6. D. Boneh, G. Crescenzo, R. Ostrovskyy,
7. G. Persianoz, “Public key encryption with keyword search”, in Eurocrypt 2004, Interlaken, Switzerland, May 2-6, 2004, pp.506-522.
8. N. Cao, C. Wang, M. Li, K. Ren, W. Lou, “Privacy-preserving multikeyword ranked search over encrypted cloud data”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222-233, Nov. 2013.
9. S. Seo, M. Nabeel, X. Ding, E. Bertino,“An efficient certificateless encryption for secure data sharing in public clouds”, IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2107-2119,Sept. 2014.
10. Gill, D. R. . (2022). A Study of Framework of Behavioural Driven Development:

Methodologies, Advantages, and Challenges. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 09–12. https://doi.org/10.17762/ijfrcsce.v8i2.2068

11. L.A. Dunning, R. Kresman, “Privacy preserving data sharing with anonymous IDassignment”, IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp.402-413, Feb. 2013.
12. X. Chen, X. Huang, J. Li, J. Ma, D. Wong, W. Lou, “New algorithms for secureoutsourcing of large-scale systems of linear equations”, IEEE Transactions on Information and Forensics Security, vol.10, no. 1, pp. 69- 78, Jan. 2015.
13. X. Chen, J. Li, J. Weng, J. Ma, W. Lou, “Verifiable computation over large database with incremental updates” IEEE Transactions on Computers, vol. 65, no. 10:3184-3195, Oct. 2016.
14. Kanyadara Saakshara, Kandula Pranathi, R.M. Gomathi, A. Sivasangari, P. Ajitha, T. Anandhi, "Speaker Recognition System using Gaussian Mixture Model", 2020 International Conference on Communication and Signal Processing (ICCSP), pp.1041-1044, July 28 - 30, 2020.
15. R. M. Gomathi, P. Ajitha, G. H. S. Krishna and I. H. Pranay, "Restaurant Recommendation System for User Preference and Services Based on Rating and Amenities," 2019 International Conference on Computational Intelligence in Data Science (ICCIDS), 2019, pp. 1-6, doi: 10.1109/ICCIDS.2019.8862048.
16. M. S. Kiran and P. Yunusova, “Tree-Seed Programming for Modelling of Turkey Electricity Energy Demand”, Int J Intell Syst Appl Eng, vol. 10, no. 1, pp. 142–152, Mar. 2022.
17. Subhashini R, Milani V, "IMPLEMENTING GEOGRAPHICAL INFORMATION SYSTEM TO PROVIDE EVIDENT SUPPORRT FOR CRIME ANALYSIS", Procedia Computer Science, 2015, 48(C), pp. 537–540
18. Harish P, Subhashini R, Priya K, "Intruder detection by extracting semantic content from surveillance videos", Proceeding of the IEEE International Conference on Green Computing, Communication and Electrical Engineering, ICGCCEE 2014, 2014, 6922469.
19. Sivasangari, A., Krishna Reddy, B.J., Kiran, A., Ajitha, P.(2020), “ Diagnosis of liver disease using machine learning models”, ISMAC 2020, 2020, pp. 627–630, 9243375.
20. Sivasangari, A., Nivetha, S., Pavithra,, Ajitha, P., Gomathi, R.M. (2020),” Indian Traffic Sign Board Recognition and Driver Alert System Using CNN”, 4th International Conference on Computer, Communication and Signal Processing, ICCCSP 2020, 2020, 9315260.
21. Ajitha, P., Lavanya Chowdary, J., Joshika, K., Sivasangari, A., Gomathi, R.M., "Third Vision for Women Using Deep Learning Techniques", 4th International Conference on Computer, Communication and Signal Processing, ICCCSP 2020, 2020, 9315196.
22. Ajitha, P.Sivasangari, A.Gomathi, R.M.Indira, K."Prediction of customer plan using churn analysis for telecom industry",Recent Advances in Computer Science and Communications,Volume 13, Issue 5, 2020, Pages 926-929.
23. Gowri, S. and Divya, G., 2015, February. Automation of garden tools monitored using mobile application. In International Confernce on Innovation Information in Computing Technologies (pp. 1-6). IEEE.
24. Ananthakrishnan, B., V. . Padmaja, S. . Nayagi, and V. . M. “Deep Neural Network Based Anomaly Detection for Real Time Video Surveillance”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 54-64,

doi:10.17762/ijritcc.v10i4.5534.

25. Gowri, S., and J. Jabez. "Novel Methodology of Data Management in Ad Hoc Network Formulated Using Nanosensors for Detection of Industrial Pollutants." In International Conference on Computational Intelligence, Communications, and Business Analytics, pp. 206-216. Springer, Singapore, 2017.
26. Nouby M. Ghazaly, A. H. H. . (2022). A Review of Using Natural Gas in Internal Combustion Engines. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 07–12. https://doi.org/10.17762/ijrmee.v9i2.365