International Journal of Computational Intelligence in Control

Accomplishing memory leakage flexibility framework utilizing physically unclonable capabilities and Fuzzy Extractor

T. Rajendran[1*]B. Karthikeyan[1]Nannuri Suresh[1]G. Sai Sravanthi [2]K. Vijay [1] P. Lakshmi Tejaswini[1]
[1]Department of Information Technology, QIS College of Engineering and Technology, Ongole, India
[2]Department of ECE, QIS College of Engineering and Technology, Ongole, India
*Corresponding Author: T. Rajendran&it.hod@qiscet.edu.in

ABSTRACT: -Offloading private information to shared cloud storage and letting end users perceive that data as the best choice for a wide range of users, giving people more flexibility and lower prices. For security reasons, private data should be encrypted before offloading, making traditional keyword search tactics impractical. As such, searchable.Cryptography has been extensively researched in recent years. For practicality, multi-keyword ranked searches on encrypted data are important. However, almost all existing multiple keyword ordering search schemes suffer from the security threat of non-volatile memory leak attacks. To solve this kind of problem, a secure multi-keyword gradient search scheme is proposed that resists memory leak attacks. The executed plan utilizes genuinely irreproducible capabilities (PUFs) to change watchwords and report identifiers. Due to the noisy nature of PUF, we usea Fuzzy Extractor (FE) to recover the key of the key.

Index Terms—Shrewd body sensor organization, precise encryption, unclonable usefulness, accessible encryption.

I. INTRODUCTION

As the amount of data grows dramatically, one possible solution is to have it stored on remote servers in the cloud, where it can be accessed cheaply, efficiently, and with minimal effort on the user's part. There are also practical considerations, since the large volume of data collected by smart body sensors is beyond the capabilities of most of these devices to analyse and store. Encrypting data before outsourcing prevents unauthorised access. Searching encrypted data is difficult with this encrypt-then-outsource technique. Since Tune et al. [1] first proposed accessible encryption, it has been widely explored. This is exhibited by the few frameworks with different highlights that have been presented in the writing.

Single watchword [2, 3], numerous catchphrase [4, 5], fluffy and likeness [11, 12], dynamic [14, 15], positioned [16-19], different client [20], and unquestionable [21, 22] pursuits are models.There is notyet a scheme that can fully realise all of these capabilities, albeit [25] besides, because of the rise of new assaults, developing new accessible encryption frameworks with different security aspects is generally fundamental. One kind of side- channel attack is a memory leak-age attack,in which the attacker tries to steal secret keys by probing memory itself.

Arm knecht et al. [24] in 2009 proposed a cryptographic crude in view of truly unclonable capabilities (PUFs) to endure such an assault. Pseudorandom sequences can be generated with this primitive, and it can also be utilised in pseudorandom functions. On the basis of this basic, they developed a block cypher that is secure against both algorithmic and physical attacks, as well as memory attacks. At present Web of Things (IoT) gadgets, like savvy body sensors, can have this component added or worked in to assist with protecting confidential data(for example wellbeing and clinical related in-line).

The security of encryption keys is paramount for any method that can be decrypted by a search engine. According to a 2002 paper by Pappu et al. [25], PUF can be used to safely generate secrets by exploiting physical properties inherent to devices. Memory that doesn't leak searches. In 2016, Dai et al. [21] provided a traditional definition of secure-key encryption(SSE). They created two PUF- based SSE algorithms that are immune to memory leaks. However, their approaches are limited to keyword searches and cannot perform any sort of rating or verification. To accommodate multi-keyword ranked searches, Chen et al. [22] improved the algorithm of Dai et al (MRSS-ML).

In contrast to the methodology in [22], the strategy proposed in this paper uses a vector space model to assess the consistency of search results. It also makes it easier to check the integrity of encrypted data and allows for real-time data updates. The primary benefits of the proposed system include: We foster a dynamic and certain multi-catchphrase positioned search plot that can be utilized on encoded information from a savvy body sensor organization. As far as we could possibly know, this is the main way to deal with at the same time accomplish these three objectives.

The present strategy beats the multi-watchword positioned search (MRSE) method gave in [5] to large information assortments in tests. We exhibit MLR-DVMRS security. Segments 2 and 3 examine comparable work. Area 4 covers framework and security models. The fifth area portrays our methodology. Areas 6 and 7 incorporate security and execution assessment. Segment eight finishes up.

II. RELATED WORK

A single-keyword SSE method was proposed by Song et al. [2]. There are many methods and techniques that can be used to supplement the search function and increase search accuracy. A few models include: multi-catchphrase search [6-7], fluffy and closeness search [8-11], unique hunt [12-13], multi-user search [14], ranked search [15-16], and verifiable search [17-18].

Cao et al. [6] presented a solid multi-watchword positioned search (MRSE) framework in which "coordinate matching" and "inner product similarity" similarity measures were combined to quantitatively evaluate such similarity measures. This technique can convey query items positioned as per the quantity of matched terms. Be that as it may, MRSE doesn't consider the recurrence of catchphrase access. Two dense matrices encrypt the secure list and secret entryway for the record vector and question vector in MRSE.When the number of keywords in a dictionary continuously increases, the performance of scalar products will be dramatically diminished. After the keyworddictionary is created, the vector structure cannot be changed since keywords are ordered. Chen et al. [7] developed an effective dynamic multi-keyword ranked search (DMRS) technique that replaces dense matrices in index construction andtrapdoor generation with sparse block matrices. It will considerably save computer resources.. In DMRS, the dynamic update action of the document is implemented using a reverse configuration.

A powerful symmetric accessible encryption which was by introduced Gajek [12] from constrained functional encryption schemewith dynamic symmetric searchable encryption, where the proposed scheme could realize logarithmic search efficiency within the size of keyword set and is proved to be secure supported the subgroup decision problem in bilinear groups.

Yang et al. [13]for cloud-based e-health applications in which users' individual health data is created and saved on a regular basis, we developed a zealous and adaptable SSE architecture. Secure and proficient multi-catchphrase similitude accessible encryption (MKSim) was proposed by Strizhov and Ray [14], bringing searchable encryption into a multi-user context. It can be proven safe against adaptive chosen-keyword attacks. (CKA2-secure) within the random oracle model. Zhang et al. [16] presented a secure ranked multi-keyword search scheme during a multi-owner model (PRMSM).

The majority of the searchable encryption schemes were compiled by Wu et al. [19], who also performed individual contribution analysis. In their recent article, Poh et al. [20] surveyed the landscape of the many SSE programmme now in use. They offered an SSE event summary and elaborated on SSE constructs to back up the proposed overarching framework. They looked at how different architectures measured up in terms of overall search performance, security approaches, and other features and capabilities. The studies were backed by an analysis of the obstacles and recommendations for further study.

All SSE systems assume that the data owner has a private key that the attacker cannot access. Unfortunately,attackers often use side-channel attacks to steal a knowledge owner's private key. These attacks compromise all SSE schemes. A binary vector indicates the index and trapdoor in MRSE scheme [6]. The document or query's keyword presence.To ensure the confidentiality of our proposed scheme, the document what'smore, question vectors are scrambled by multiplying two dense matrices. In addition, the search term similarity value, that is, the document similarity value, isjumped at each subindex by trapdoor's scalar product. Note that the keys, ie the two dense matrices, must be properly storedin their own non-volatile memory. However, the owner's persistent disk can be attacked by a potential attacker within your cloud storage environment..

Multi-keyword ranked search and non-volatile memory leakage resistance, we improve the MLR-SSE scheme to include the multi-catchphrase comparability search and propose a protected multi-watchword positioned search plot (MRSS-ML). The file development of MRSS-ML is improved from the plan proposed in [14] which is predicated on SSE-2 rearranged record information development recentlypresented in [21]. So as to understand the upper security requirements, keywords or document identifiers are randomized by a physically unclonable function (PUF).

Because of the uproarious impact of PUFs, the fluffy extractor is decided to recuperate the keys. Moreover, a similarity score table is made to realize the functionality of multi-keyword ranked search. Furthermore, the request safeguarding capability [16] is improved to monitor the protection of closeness among watchwords and reports. These procedures create a memory leakage-resistant multi-keyword ranked search strategy (MRSS-ML)..

III. SYSTEM MODEL

Figure 1 shows that MRSS-ML has three separate parts. People who own information, people who use information, and cloud servers. The owner of the information wants to give the cloud server the collection of documents D. First, wetake a collection of keywords W' from Dand add some fake keywords to a dictionaryof keywords W. Next, make a searchable encrypted index I from collection D, encrypt each document in collection D, and get a collection C of encrypted documents. Lastly, send the encrypted index I and collection C to the cloud server. A data user is an entity that has been given access to the documents of the data owner. A cloud server stores a list of encrypted documents and an encrypted index that can be searched. You have to look through the encrypted index and give the user the top k most important encrypted documents.

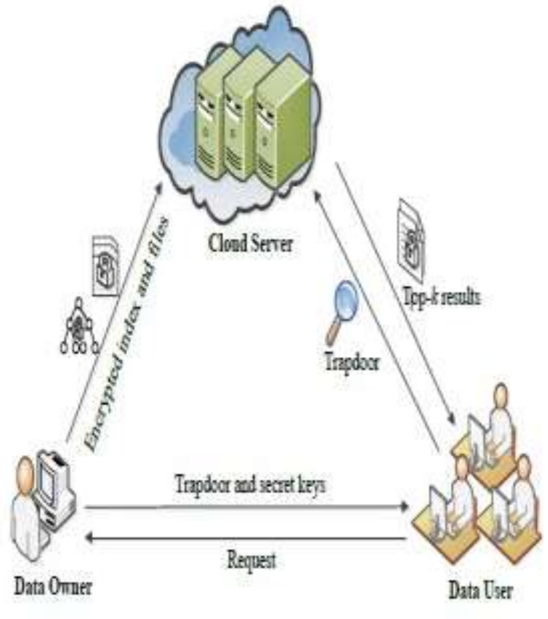

Fig. 1. System Model.

Date owner:

The data proprietor makes and encodes the accessible record and archives. He stores encoded papers and record on the cloud server. Edge or haze figuring hubs execute encryption since the shrewd body sensor might be asset limited.

Data user:

In the suggested approach, it is assumed that the data user is trustworthy. If the user needs specific data (such his or her parents' medical history), s/he can submit a request for information to the data's owner. The data proprietor transfers the fundamental data to the client to acquire the mysterious path as per the picked security strategy. Data users would obtain encrypted files corresponding to their queries after passing the trapdoor to the cloud server..

Cloud server:

Cloud servers store encrypted documents and indexes. This shows cloud servers may remove data to save storage and management value. Returning incomplete search results. Thus, cloud server search results and encrypted data must be verified. However, the cloud server must follow protocol. The cloud server directs theinquiry calculation and gives encoded records comparing to the question catchphrases to the information client subsequent to getting the approval.

IV. SECURITY MODEL

This section introduces the whole non-volatile memory attack paradigm.

Definition1. (NVMA [22]):

S is data owner's nonvolatile memory's secret. Assume α is a function that: α(x) x, x < N. The attack oracle O adaptively chooses a polynomial-size attack function g(•) and outputs g(S) with a maximum number of bits of α(|S|) for a non-volatile memory attacker A.

Definition2. (Full Non-unstable Memory Assault):

An assault model is full non-unpredictable memory attack if an assailant A meets Definition 1 and α = id characterized in[22].

Customary assault models accept that an assailant can't get to data about keys put away in non-unstable memory. Clearly, in a real-world environment, this assumption is unreasonable. For security reasons, do not store long-term secrets in non-volatile memory.

Fortunately, the physical non-cloning functions presented in [3] that don't need to be stored are often used to generate keys in real time. Therefore, an attacker would not want to obtain information about keys stored in non-volatile memory.

FUZZY EXTRACTOR

Due to thermal noise and ambient variables, PUF response r isn't perfectly reproduced. Raw answers cannot be used as cryptographic keys. PUF key generators may generate full-bit-entropy cryptographic keys from responses r. Key generators often use secure sketch and entropy extraction. Fuzzy extractor (FE) [23]–[24]. Error correction uses assistance data to adjust noisy responses. Code-offset and syndrome construction are two common secure sketch techniques for fuzzy extractors [23]. This study uses syndrome-based building, briefly discussed here..

Gen and Rep are secure sketch capabilities (). Key enlistment creates aide information p, where p = r × HT and H might be an excess check network of a straight blunder adjustment code. The key recreation Rep(r 0,p) first develops a disorder, s = (r 0 × HT) x p = e x HT, with e a mistake vector. A misstep area calculation decides e. r = e - r 0. An entropy extraction technique like an all inclusive hash capability might be required if the recuperated PUF reaction r isn't consistently dispersed. packs the PUF reaction into a cryptographic key with full piece entropy.

The server computes optional data using the Gen() method during fuzzy extractor deployment. The field executes Rep(). Van Herrewege et al. edited. [35] Gen() on a token with restricted resources while transmitting computationally complex execution to powerful servers. "Reverse Fuzzy Extractor" describes this approach (RFE).

Order-preserving function

Order preserving function (OPF) encoding protects the similarity score against attackers. [16] improves OPF formalisation.

The request safeguarding capability f(x)=1•i•ai•h(x, i)+r might be an irregular number that protects the capability from the cloud server. h(x, I)β and are constants. r should satisfy (0, 2 - 1) to ensure positioned results. [16] characterizes, hypotheses, and demonstrates OPF.

The safety Analysis

From the past depiction, a few sham catchphrases are embedded into the file, which is utilized to keep watchword recurrence investigation from the likely assailants. The record assortment is scrambled by symmetric encryption calculation.since the attackers cannot learn anything about documents if the encryption algorithm is secure. We mainly specialize in analyzing the safety of index, trapdoor and search pattern as follows.

V. CONCLUSION

This article proposed an alternative, secure method of conducting multiple-keyword searches. Designed to prevent memory leak attacks, this method permits real-time updates to indexes and data as well as integrity checks to ensure data consistency. The suggested schema differs from the MRSS-ML schema in that it constructs a lookup table to locate candidate document identifiers that match the keywords requested, as well as a score table and scores them according to multiple keywords.

A fuzzy extractor and four PUFs are also utilized to make the search more resistant to memory leaks. Additionally, OPE is employed to encode relevance ratings for ranked search. Using vector models and Mac functions, we modify the index construction and check the outcomes using both. The experimental evidence demonstrates the adequacy and feasibility of the proposed approach.. The next step will be to develop prototypes of the suggested scheme and to collaborate with real-world network operators of smart bodysensors.

VI. REFERENCES

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, Public Key Encryption with Keyword Search, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004, pp. 506-522.

[2] D. X. Song, D. Wagner, A. Perrig, Practical Techniques for Searches on Encrypted Data, IEEE Symposium on Security and Privacy, Berkeley, California, 2000, pp. 44-55.

[3] S. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical One- way Functions, Science, Vol. 297, No. 5589, pp. 2026-2030, September, 2002.

[4] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy Extractors: How to Generate Strong Keys from iometrics and Other Noisy Data,SIAM Journal on Computing, Vol. 38, No. 1, pp. 97-139, March, 2008.

[5] S. Dai, H. Li, F. Zhang, Memory Leakage-resilient Searchable Symmetric Encryption, Future Generation

Computer Systems, Vol. 62, pp. 76-84, September, 2016.

[6] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, pp. 222-233, January, 2014.

[7] L. Chen, L. Qiu, K. C. Li, W. Shi, N. Zhang, DMRS: An efficient Dynamic Multi-keyword Ranked Search Over Encrypted Cloud Data, Soft Computing, Vol. 21, No. 16, pp.4829-4841, August, 2017.

[8] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, W. Lou, Fuzzy Keyword Search over Encrypted Data in Cloud Computing, The 29th Conference on Computer Communications, San Diego, CA, 2010, pp. 1-5.

[9] (Efpso-Wc) and Gene Ontology for Microarray Gene Expression."*In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing, pp. 48-55. 2018.* *https://dl.acm.org/doi/abs/10.1145/3299852.3299866*

[10]C. Narmatha , Dr. M. Thangamani , S. Jafar Ali Ibrahim, “Research Scenario of Medical Data Mining Using Fuzzy and Graph theory”, *International Journal of Advanced Trends in ComputerScience and Engineering, Vol 9, No 1 (2020): 349-355,* https://doi.org/10.30534/ijatcse/2020/52912020, https://www.warse.org/IJATCSE/static/pdf/file/ijatcse52912020.pdf

[11] Jafar Ali Ibrahim. S, Mohamed Affir. A *“Effective* Scheduling of Jobs Using Reallocation of Resources Along With Best Fit Strategy and Priority”, International Journal of Science Engineering and Advanced Technology(IJSEAT) – ISSN No: 2321-6905, Vol.2, Issue.2, Feb-2014, http://www.ijseat.com/index.php/ijseat/article/view/62

[12] **Dr**.R.Chinnaiyan , M.S.Nidhya (2018), “ ReliabilityEvaluation of Wireless Sensor Networks using EERN Algorithm” , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[13] Dr.R.Chinnaiyan , R.Divya (2018), “ Reliable AI Based Smart Sensors for Managing Irrigation Resources in Agriculture” , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[14] Dr.R.Chinnaiyan , S.Balachandar (2018) , “ Reliable Digital Twin for Connected Footballer” , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[15] Dr.R.Chinnaiyan , S.Balachandar (2018) , “ Centralized Reliability and Security Management of Data in Internet of Things (IoT) with Rule Builder” , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[16] Dr.R.Chinnaiyan, Abishek Kumar (2017) “ Reliability Assessment of Component Based Software Systems using Basis Path Testing” , IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 512 – 517

[17] Dr.R.Chinnaiyan, Abishek Kumar (2017) “ Reliability Assessment of Component Based Software Systems using Basis Path Testing” , IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 512 – 517

[18] Dr.R.Chinnaiyan, Abishek Kumar(2017) ,”Construction of Estimated Level Based Balanced Binary Search Tree”, 2017 IEEE International Conference on Electronics,Communication, and Aerospace Technology (ICECA 2017), 344 - 348, 978-1-5090-5686-6.

[19] Dr.R.Chinnaiyan, Abishek Kumar(2017), Estimation of Optimal Path in Wireless Sensor Networks based on Adjancy List, 2017 IEEE International Conference on Telecommunication,Power Analysis and Computing Techniques (ICTPACT2017) ,6,7,8th April 2017,IEEE 978-1-5090-3381

[20] Dr.R.Chinnaiyan, AbishekKumar(2017) ,”Construction of Estimated Level Based Balanced Binary Search Tree”, 2017 IEEE International Conference on Electronics,Communication, and Aerospace Technology (ICECA 2017), 344 - 348, 978-1-5090-5686-6.

[21] Dr.R.Chinnaiyan, AbishekKumar(2017), Estimation of Optimal Path in Wireless Sensor Networks based on Adjancy List, 2017 IEEE International Conference on Telecommunication,Power Analysis and Computing Techniques (ICTPACT2017) ,6,7,8th April 2017,IEEE 978-1-5090-3381-2.

[22] Dr.R.Chinnaiyan, R.Divya (2017),” Reliability Evaluation of Wireless Sensor Networks”, IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 847 – 852

[23] Dr.R.Chinnaiyan, Sabarmathi.G (2017),” Investigations on Big Data Features , Research

Challenges and Applications", IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 782 – 786

[24] G.Sabarmathi , Dr.R.Chinnaiyan (2018), "Envisagation and Analysis of Mosquito Borne Fevers – A Health Monitoring System by Envisagative Computing using Big Data Analytics" in ICCBI 2018 – Springer on 19.12.2018 to 20.12.2018 (Recommended for Scopus Indexed Publication IEEE Xplore digital library)

[25] G.Sabarmathi , Dr.R.Chinnaiyan, Reliable Data Mining Tasks and Techniques for Industrial Applications, IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES, VOLUME 4, ISSUE 7, DEC/2017,PP-138-142, ISSN NO: 2394-8442

[26] Ibrahim, Mr S. Jafar Ali, K. Singaraj, P. Jebaroopan, and S. A. Sheikfareed. "Android Based Robot for Industrial Application." International Journal of Engineering Research & Technology 3, no. 3 (2014).

[27] Ibrahim, S. Jafar Ali, and M. Thangamani. "Momentous Innovations in the Prospective Method of Drug Development." In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing, pp. 37-41. 2018.

[28] Ibrahim, S. Jafar Ali, and M. Thangamani. "Prediction of Novel Drugs and Diseases for Hepatocellular Carcinoma Based on Multi-Source Simulated Annealing Based Random Walk." Journal of medical systems 42, no. 10 (2018): 188. https://doi.org/10.1007/s10916-018-1038-y ISSN 1311-8080, https://acadpubl.eu/hub/2018-119-16/1/94.pdf

[29] Jafar Ali Ibrahim. S, Mohamed Affir. A "Effective Scheduling of Jobs Using Reallocation of Resources Along With Best Fit Strategy and Priority", International Journal of Science Engineering and Advanced Technology(IJSEAT) – ISSN No: 2321- 6905, Vol.2, Issue.2, Feb-2014, http://www.ijseat.com/index.php/ijseat/article/view/62

[30] M. Thangamani, and Jafar Ali Ibrahim. S, "Knowledge Exploration in Image Text Data using Data Hiding Scheme," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, 14-16 March, 2018, Hong Kong, pp352-357 http://www.iaeng.org/publication/IMECS2018/IMECS2018_pp352-357.pdf

[31] M. Thangamani, and Jafar Ali Ibrahim. S, "Knowledge Exploration in Image Text Data using Data Hiding Scheme," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, 14-16 March, 2018, Hong Kong, pp352-357 http://www.iaeng.org/publication/IMECS2018/IMECS2018_pp352-357.pdf

[32] R.Chinnaiyan, S. Somasundaram (2011) ,"An SMS based Failure Maintenance and Reliability Management of Component Based Software Systems", European Journal of Scientific Research, Vol. 59 Issue 1, 9/1/2011, pp.123 (cited in EBSCO, Impact Factor: 0.045)

[33] R.Chinnaiyan, S.Somasundaram (2012) , Reliability Estimation Model for Software Components using CEP", International Journal of Mechanical and Industrial Engineering (IJMIE) , ISSN No.2231-6477, Volume-2, Issue-2, 2012, pp.89-93.

[34] R.Chinnaiyan, S.Somasundaram(2010) "Evaluating the Reliability of Component Based Software Systems " ,International Journal of Quality and Reliability Management , Vol. 27, No. 1., pp. 78-88 (Impact Factor: 0.406)

[35] R.Chinnaiyan, S.Somasundaram(2011), "An Experimental Study on Reliability Estimation of GNU Compiler Components - A Review", International Journal of Computer Applications, Vol.25, No.3, July 2011, pp.13-16. (Impact Factor: 0.814)

[36] S. Jafar Ali Ibrahim and M. Thangamani. 2018. Momentous Innovations in the Prospective Method of Drug Development. In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing (DMIP '18). Association for Computing Machinery, New York, NY, USA, 37–41. https://doi.org/10.1145/3299852.3299854

[37] S. Jafar Ali Ibrahim and Thangamani, M "Proliferators and Inhibitors Of Hepatocellular Carcinoma", International Journal of Pure and Applied Mathematics (IJPAM) Special Issue of Mathematical Modelling of Engineering Problems Vol 119 Issue. 15. July 2018

[38] Thangamani, M., and S. Jafar Ali Ibrahim. "Ensemble Based Fuzzy with Particle Swarm Optimization Based Weighted Clustering (Efpso-Wc) and Gene Ontology for Microarray Gene Expression." In Proceedings of the 2018 International Conference on Digital Medicine and Image Processing, pp. 48-55. 2018. https://dl.acm.org/doi/abs/10.1145/3299852.3299866