Confidential data sharing in cloud with secured IOT Assistance

M. Hemasri[a], J. Amrita[b], S. Shri Sakthi[c], M. Sruthi[d], and S. Yuvashreee[e]
[a]
Department of Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India - 639113
[b,c,d,e] Department of Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India - 639113

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: The always developing number of Internet associated gadgets represents a few network safety chances. A large portion of the traded information between the Internet of Things (IoT) gadgets are not enough gotten because of asset limitations on IoT gadgets. Quality Based SignCryption (ABSC) is an incredible cryptographic system reasonable for dispersed conditions, giving adaptable access control and information mystery. Be that as it may, it forces high plan grave particle costs, and doesn't uphold access strategy update (client expansion/disavowal). This paper presents PROUD, an ABSC arrangement, to safely re-appropriate information design cryption cycle to edge workers to diminish the calculation overhead on the client sides. Pleased permits end-clients to offload the vast majority to an edge worker and check the accuracy of the got halfway design crypted information from the edge worker. The entrance strategy update include in PROUD doesn't influence the size of the message got by the end customer which decreases the information move limit and the limit purposes. Our complete hypothetical, trial investigation demonstrates that the beats existing plans regarding usefulness, correspondence and calculation.

Keywords: Attribute Based Signcryption, Access policy update, and Outsourced designcryption Cloud assisted IoT, Privacy Confidentiality Access control Anonymous data origin authentication

1. Introduction

With the quick headway of frameworks organization and PDAs, we are facing a dangerous incensement of openly upheld data from countless customers. These openly upheld data can be added up to dynamically and mined by AI developments to discover critical information and further benefit our life. Actually a steadily expanding number of associations are distributed the openly upheld data to individuals overall for data mining purposes. Nevertheless, the promising central marks of data appropriating and mining are at the risk of revealing sensitive information to data diggers.

All these current systems base on using cryptography or differential security to scramble or trouble unrefined data on the data benefactor, which can guarantee the certifiable data freely, anyway isn't sensible for the protection of all out estimations over openly upheld data, since the inconvenience of rough data on each customer would not impact the estimation assessment over openly upheld data. Furthermore, all current computations under an untrusted worker can't give strong confirmation to steady data conveying. These issues energize us to structure another differentially private framework for ceaseless freely upheld quantifiable data appropriating with the untrusted worker.

In the first place, how to add up to over openly upheld data without a central trusted in worker? Exactly when the worker is known as untrusted, each customer would not exchange the enlistment information to the worker explicitly any more, which makes it difficult to get the amassed bits of knowledge for dissemination. Second, how to ensure the assurance of each individual? The primary one that can be trusted by a customer is itself. Regardless of the way that a customer should move its enlistment information to some place with the ultimate objective of mixture, its character should be concealed so the moved data would be not associated with the customer as mentioned in figure 1.1. At last, without a central trusted in worker, the insurance spending will undoubtedly be assigned and used distributed instead of a central way. As such, it is attempting to recognize w-event differential security for the steady released data without a central trusted in worker.

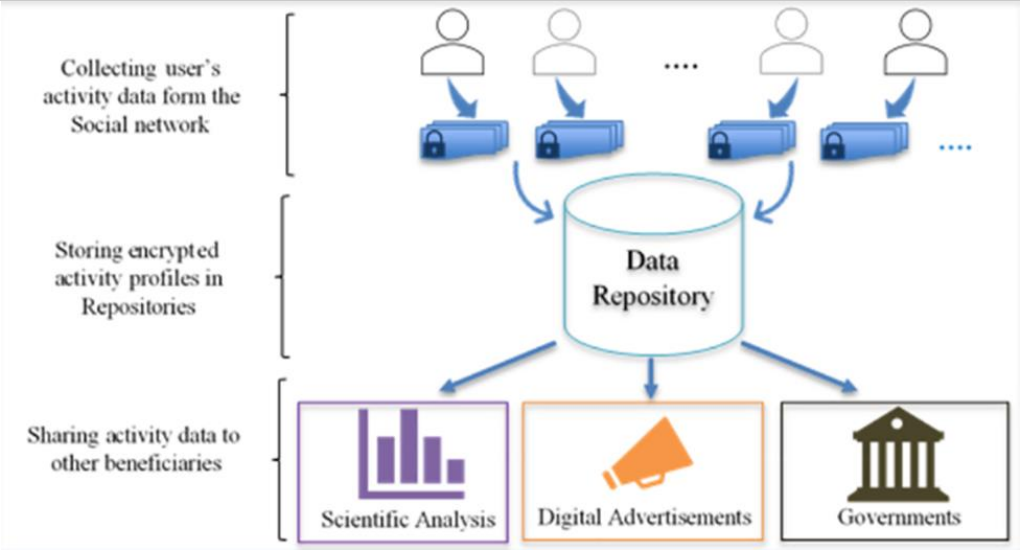

Figure 1.1: Anomaly detection over differential preserved privacy in online

2. Cloud Computing

Cloud computing is a processing worldview, where an enormous pool of frameworks is associated in private or public organizations, to give progressively adaptable foundation to application, information and record accumulation.

Figure 1.1: Conceptual view of cloud computing

In existing framework has been executed utilizing generally depend on a confided in worker to total the spatio-fleeting publicly supported information and afterward apply differential security instrument to annoy the total insights prior to distributing to give solid protection check.

Be that as it may, the protection of clients will be uncovered once the worker is hacked or can't be trusted.

sIn this undertaking, we propose an adaptable security saving information sharing (FPDS) plot in cloud-helped IoT. With the FPDS plot, an IoT client can encode information to a beneficiary by utilizing character based encryption. All the more critically, the IoT client can determine a fine-grained admittance strategy to create an appointment accreditation, and afterward send this certification to the cloud so it can change over all the scrambled information fulfilling the entrance strategy into new ciphertexts that are meaningful to another beneficiary. Thusly, IoT clients can share the information moved to the cloud in an adaptable and protection saving way.

The proposed framework IOT based cloud helped Security plot actualized for security reason.

The proposed framework comprises of confirmation focus (AC), cloud specialist organization (CSP), information proprietors and information customers.

The proposed framework give the common security between we focus on the new protection issues brought about by the commonality between the passage and the cloud, and preclude the classification of information imparted among the IoT gadgets.

3. Literature Survey

[1] Standard available encryption plans license customers to securely investigate mixed data through watchwords, these methods maintain simply boolean chase, without getting any meaning of data records. This philosophy encounters two guideline disservices when clearly applied inside the setting of Cloud Computing. Customers, who do not actually has pre-data on mixed cloud data, association each recuperated enter solicitation to look out ones most planning their benefit, unexpectedly hand, continually recuperating all records containing the examined watchword further brings regarding unnecessary association traffic is terrible in the current cloud perspective.

[2] have said a twofold significant count (DPDCM) for colossal data feature acknowledging, which stretches out the rough commitment in the mysterious layers to learn associated features of huge data by replacing the mysterious layers of the normal significant estimation.

[3] hinder unapproved data use, induction control is fundamental in multiple customer system. Regardless, affirmed customer may deliver the puzzling key for money related benefit. Thusly, following and denying malignant customer who mauls secret key ought to be tended to definitely

[4] an ABE scheme with reconsidered unscrambling grants an untouchable to change El Gamal-type ciphertext using a public key given by a customer so the last can be decoded altogether more beneficially than the past by the customer. Regardless, a disadvantage of the first reevaluated ABE contrive is that the rightness of cloud specialist's change can't be checked by the customer.

[5] an adaptively secure character based transmission encryption structure featuring consistent estimated ciphertext in standard. The public key and the private keys of our structure are both direct in the most outrageous

number of recipients. Furthermore, our structure is totally understanding safe and has stateless beneficiaries. Differentiated and the top tier, our arrangement is a lot of cutting edge for the transmission encryption.

[6] System which beats essentially all of the flaws of the KNN-SE that is based MRSE structures. New structure needn't bother with a predefined watchword expressions in optional lingos, is a multi-customer system which maintains versatile pursuit endorsement repudiation, and it achieves better data security affirmation cloud specialist can't told which records are the top-k results back to a data customer. We similarly direct expansive preliminaries to display the viability of the new structure.

[7] open public key encryption engages a limit laborer to recuperate the uninhibitedly mixed data without uncovering the principal data substance. It offers an ideal cryptographic response for mixed data recuperation in encoded data amassing structures. Certificateless cryptography (CLC) is a novel cryptographic rough that has various advantages. It vanquishes the issue in character based cryptosystems and the cumbersome confirmation in standard public key cryptosystems. Prodded by the drawing in features of CLC, three certificateless encryption with expression search (CLEKS) plans were presented in the composition. Regardless, all of them were worked with the costly bilinear mixing and henceforth are not sensible for the devices that have limited enrolling resources and battery power.

[8] Secure offer and mission reconsidered data is a monumental task, adequately achieve the spillage of delicate individual information. Beneficial data and looking with security is of essential importance. Now the paper, strangely, proposes an available quality based go-between reencryption structure. At the point when differentiated and the current structures simply supporting either available trademark based handiness or quality based go-between reencryption, our new unrefined sponsorships the two limits and gives versatile watchword update organization. The system engages a data to adequately give his data to a predefined assembling of customers organizing a sharing plan and afterward, the data will keep up its available property yet.

[9] another perspective for ABE that by and large slaughters this overhead for customers. Expect that ABE ciphertexts are taken care of in the cloud. We show how a client can give the cloud a solitary change key that permits the cloud to unravel any ABE ciphertext fulfilled by that client's credits into a (reliable size) El Gamal-style ciphertext, without the cloud having the decision to examine any piece of the client's messages

[10] a client gives an untrusted worker, say a cloud master relationship, with a change key that permits the cloud to unravel any ABE ciphertext fulfilled by that client's credits or access strategy into a reasonable ciphertext, and it commendable inspirations to some degree computational overhead for the client to recuperate the plaintext from the changed ciphertext. Security of an ABE framework with rethought unscrambling guarantees that an adversary (counting a toxic cloud) won't learn anything about the blended message; notwithstanding, it doesn't ensure the precision of the change done by the cloud. In this paper, we consider another fundamental of ABE with reevaluated unscrambling: confirmation. Casually, sureness ensures that a client can competently check if the change is done accurately.

[11] an inadequacy of the first rethought ABE conspire is that the accuracy of the cloud worker's change can't be checked by the client. In here this paper, we initially formalize a privact model of ABE with undeniable re-appropriated decoding by presenting a confirmation key in the yield of the encryption calculation.

[12] characterize and build a component that empowers us to give a key to the passage the doorway to test whether "dire" is a watchword in the email without getting the hang of whatever else about the email. They have alluded to this system as Public Key Encryption with catchphrase Search.

[13] another framework that underpins arrangements communicated in any droning access structures. Additionally, the proposed framework is just about as proficient and protect as truly outstanding (non-recognizable) CP-ABE frameworks as of now accessible, that is, this work adds recognizability to a current expressive, effective, and secure the CP-ABE conspire without debilitating its privacy or setting a specific compromise on its exhibition.

[14] capacity of ABE to follow the noxious clients or swindlers who purposefully release the incomplete or adjusted decoding keys for benefits. By the by, because of the idea of CP-ABE, it is hard to distinguish the first key proprietor from an uncovered key since the unscrambling advantage is shared by various clients who have similar ascribes. Then again, A few frameworks have been proposed to acquire both of the properties. Nonetheless, none of them accomplish the 2 properties at the same time practically speaking, which restricts the business utilizations of CP-ABE partially.

[15] the plan is likewise specifically recognizable against strategy explicit unscrambling blackbox. Moreover, and all the more significantly, we demonstrate an overall explanation that if a CP-ABE plot is (specifically) recognizable against strategy explicit decoding blackbox.

[16] to assemble a framework that underpins rich arrangement of inquiry. In our installment door model one can envision examination inquiries, for example, (esteem > 1000) or even conjunctions, for example, (esteem > 1000) and (TransactionTime > 5pm). The entryway ought to get familiar with no data other than the estimation of the conjunctive predicate.

[17] it permits an outsider knowing the hunt secret entryway of a catchphrase to look through scrambled archives containing that watchword without unscrambling the reports or knowing the catchphrase. In any case, the watchword will be undermined by a noxious outsider under a catchphrase surmise assault (KGA) if the catchphrase space is in a small size.

[18] permitting a client to re-appropriate her scrambled information to a cloud worker and representative the last to look for her sake. These plans don't qualify as a safe and adaptable answer for the multiparty setting, where clients re-appropriate their scrambled information to a cloud worker and specifically approve each other to look. Because of the likelihood that the cloud worker may connive for certain vindictive clients, it is a test to have a protected and versatile multiparty accessible encryption (MPSE) plot

[19] Says that the protection and privacy of the delicate individual data significant worries of the clients, turn of events and broadly appropriation of the frameworks. The accessible encryption (SE) conspire is an innovation to fuse security insurance and good operability works together, which can assume a significant part in the e-wellbeing record framework.

[20] problem of conjunctive of subset watchwords search work, look at the disadvantages about the having plans, and a while later give out a more compelling improvement of Public Key Encryption with Conjunctive-Subset Keywords Search (PECSK) plot. A connection with various plans about capability will be presented.

[21] In Shao's PRES plot, the intermediary can re-encode ciphertext. While in our CPRE-CKS proposition, the intermediary can just re-scramble those subsequent level code messages which contain the relating watchwords. We provide the clarity and security model for CPRE-CKS, and propose a solid plan and demonstrate its security. (3) On the best approach to build a safe CPRE-CKS conspire, we found a defect in the security verification of Hwang et al'ss. public encryption with conjunctive catchphrase search (PECK) plot was proposed.

[22] the confusion hypothesis and some particular substance of current cryptography are presented. By investigating the connection among disorder and cryptography, a few methodologies and their structure for turbulent cryptography framework are proposed. A few rules about how to pick tumultuous frameworks and their boundaries in computerized encryption are given in detail.

[23] construes that one necessities to relinquish helpfulness for security. For example, if a client wishes to recuperate just records containing certain words, it was not recently realized the most effective method to let the data storing laborer play out the chase and answer the inquiry, without loss of data mystery. We portray our cryptographic designs for the issue of looking on encoded data and give confirmations of safety to the ensuing crypto structures. Our techniques have different critical advantages.

[24] a safe record utilized for picture recovery is developed to secure the recovery results being spilled to the noxious aggressors. From the outset, reversed file is created utilizing visual expressions of pictures and afterward scrambled dually by randomized parallel encoding and a key-based Gaussian arbitrary network separately, producing a protected file

[25] permits a gathering to re-appropriate the capacity of his information to another gathering in a private way, while keeping up the capacity to specifically look over it. Issue has been the focal point of dynamic exploration and a few security definitions and developments have been proposed. We start by assessing existing thoughts of security and propose new and more security definitions.

[26] most prompt use of SSE is to the plan of accessible cryptographic distributed storage frameworks (see [19] for a conversation) which can give start to finish security to distributed storage frameworks without forfeiting utility. Different applications incorporate the plan of chart encryption conspires and controlled exposure instruments

[27] productive SSE developments are known, past arrangements are exceptionally successive. This is primarily because of the way that, presently, the lone strategy for accomplishing sub-straight time search is the altered record which requires the inquiry calculation to get to a succession memory areas, every one of which is flighty and put away at the past area in the arrangement. Spurred by progresses in multi-center models, we have another strategy for building sub-direct SSE plans.

[28] their answer gives a sensible and commonsense compromise among execution and security by productively supporting enormous data sets at the expense of moderate and very much characterized spillage to the reevaluated worker (spillage is as information access designs, never as immediate openness of plaintext information or looked through qualities). Our plan follows a cautious interaction of exchanging security for proficiency which are both measured through thorough examination.

[29] usage exertion brought to the front a few elements overlooked by before coarse-grained hypothetical execution investigations, including lowlevel space use, I/O parallelism and goodput. We likewise acquaint a few enhancements with our hypothetically ideal development that model the model's qualities intended to defeat these elements. The entirety of our plans and enhancements are demonstrated secure and the data spilled to the untrusted worker is decisively measured.

[30] conspire permits a customer to store a bunch of scrambled records on an untrusted worker so that he can proficiently recover a portion of the encoded documents containing (or filed by) explicit watchwords keeping quiet. In this paper, we initially expand the model of SSE plans to that of obvious SSE conspires, and form the UC security

[31] Schemes for secure re-appropriating of customer information with search ability are in effect progressively promoted and conveyed. In the writing, plans for achieving this effectively are called Searchable Encryption (SE). They accomplish high proficiency with provable security by methods for a quantifiable spillage profile

[32] Indistinguishability confusion (IO) is an enormous thought, amazing enough to offer ascent to practically any known cryptographic item. Earlier up-and-comer IO developments depended on explicit suppositions on logarithmic items called multi-straight evaluated encodings. We present a nonexclusive development of lack of definition confusion from public-key useful encryption with brief encryption circuits and subexponential security.

[33] Their framework is based on a novel unique accessible encryption plot with front protection and assigned obviousness for occasionally created medical services information. While the forward protection is accomplished by keeping an expanding counter for every catchphrase at an IoT entryway, the information proprietor designated unquestionable status comes from the blend of the Bloom channel and all out message check code.

[34] A straightforward competitor single direction hash work which fulfills a semi commutative property that permits it to be utilized as an aggregator. This property permits conventions to be created in which the requirement for a believed focal authority can be dispensed with. Space-proficient appropriated conventions are given for report time stepping and for participation testing, and numerous different applications are conceivable.

[35] Cryptographic gatherers time productive information structures used to check a worth has a place with a. Notwithstanding this fame, there is at present no presentation assessment of the distinctive existing de-signs. Symmetric and awry collectors are utilized in like manner with no specific contention to help both of the plan. We expect to es-tablish the speed of each plan and their application's spaces as far as their size and the size of the qualities.

[36] The creators proposed a safe dynamic steering convention, named SDRP, which utilizes personality put together plan with matching with respect to elliptic bend. It utilizes mark and 'Message Authentication Code' calculations to give start to finish, bounce to-jump and entire course confirmations. The proposed SDRP has a few benefits over the current RSA-based secure steering arrangements.

[37] The mark framework can sign a limitless number of messages, and the mark size increments logarithmically as a component of the quantity of messages marked. Mark size in a 'average' framework may go from two or three hundred bytes to a couple of kilobytes, and age of a mark may require two or three hundred to a couple thousand calculations of the basic regular encryption work.

[38] they propose a lightweight Verifiable SSE plot, that can check accuracy , fulfillment of watchword query items acquired from SSE against a noxious worker. Our plan not just accomplishes an asymptotically effective check time and correspondence overhead, yet in addition outflanks past arrangements by and by. Additionally, our plan can productively uphold refreshes on check metadata. We officially characterize and investigate the security of our plan, and direct broad analyses on huge datasets to show the proficiency of our plan.

[39] Fundamental attributes regularly connected with this worldview in the writing. In excess of 20 definitions have been read taking into consideration the extraction of an agreement definition just as a base definition containing the fundamental qualities.

[40] we inspect the security of a notable cryptographic rough, explicitly Public Key Encryption with Keyword Search (PEKS) which is especially useful in various usages of conveyed stockpiling. Unfortunately, it has been shown that the traditional PEKS structure encounters an inborn feebleness called Keyword Guessing Attack (KGA) dispatched by the dangerous laborer.

[41] task assignment issue in remote sensor organizations (WSNs) is disseminating detecting errands sanely among sensor hubs to diminish in general force utilization and guarantee these undertakings finished before cutoff times. In this paper, we propose a delicate continuous flaw open minded errand designation calculation (FTAOA) for WSNs in utilizing essential/reinforcement (P/B) strategy to help adaptation to non-critical failure instrument.

[42] a customer can procure secret keys in numerous specialists with them acknowledging his/her credits and moreover, a focal authority is needed. Eminently, a client's personality data can be extricated from his or her some touchy credits. Subsequently, existing PPMA-ABE plans can't completely secure clients' protection as different specialists can work together to distinguish a client by gathering and investigating his credits. Also, ciphertext-strategy ABE (CP-ABE) is an additional constructions to scramble messages.

[43] We propose using these associations with outline a dynamic "Social Cloud", hence enabling customers to share heterogeneous resources inside the setting of a casual local area. Moreover, the normal socially therapeutic segments (impulses, disincentives) can be used to engage a Cloud based construction for long stretch contribution to cut down assurance concerns and security overheads than are accessible in standard Cloud conditions. As a result of the original thought of the Social Cloud, a social business place is proposed as a techniques for controlling sharing.

[44] Subsequently, enabling public auditability for disseminated capacity is of essential importance so customers can depend on an outcast evaluator (TPA) to check the reliability of re-appropriated data and be clear. To securely introduce a reasonable TPA, the assessing communication should get no new shortcomings toward customer data insurance, and familiarize no extra online load with customer. In this paper, we propose an ensured disseminated capacity system supporting security saving public investigating. We further loosen up our result to engage the TPA to perform audits for various customers meanwhile and capably. Wide security and execution assessment show the proposed plans are provably secure and significantly viable.

[45] The inspiration driving the paper is to give an overall security perspective of Cloud enrolling with the plan to highlight the security stresses that should be properly tended to and sorted out some way to comprehend

the most extreme limit of Cloud preparing. These server farms might be situated in any piece of the world past the span and control of clients, there are diverse security and protection moves that should be perceived and tended to. Likewise, one can never keep the chance from getting a worker breakdown that has been seen, rather frequently in the new occasions

[46] In circulated registering, data owners have their data on cloud laborers and customers (data purchasers) can get to the data from cloud laborers. In view of the data reevaluating, regardless, this new perspective of data encouraging organization in like manner presents new security challenges, which requires a self-governing evaluating organization to check the data decency in the cloud. Some current inaccessible dependability checking procedures can simply serve for static record data and, thusly, can't be applied to the examining organization snce the data in the cloud can be logically revived.

[47] when a customer is repudiated from the social occasion, the squares, which were as of late supported by this denied customer ought to be re-embraced by a current customer. The immediate method, which allows a current customer to download the contrasting piece of shared data and re-sign it during customer repudiation, is inefficient due to the enormous size of shared data in the cloud. In this paper, we propose a novel public reviewing part for the reliability of granted data to viable customer denial at the highest point of the need list.

[48] the cloud affirms the realness of the game plan without understanding the customer's character before taking care of data. Our arrangement furthermore has the extra component of access control wherein simply significant customers can decipher the set aside information. The arrangement thwarts replay attacks and supports creation, change, and scrutinizing data set aside in the cloud. We also address customer repudiation.

[49] information imparting to countless members should consider a few issues, including productivity, information trustworthiness and protection of information proprietor. Ring mark is a promising contender to develop a mysterious and valid information sharing framework. It permits an information proprietor to secretly validate his information which can be placed into the cloud for capacity or investigation reason

[50] They portray new open key cryptosystems that produce consistent size ciphertexts with the ultimate objective that capable arrangement of unscrambling rights for any course of action of ciphertexts are possible. The peculiarity is that one can add up to any course of action of mystery keys and make them as traditionalist as a lone key, yet wrapping the power of the general large number of keys being amassed. In that capacity, the strange key holder can convey a predictable size absolute key for versatile choices of ciphertext set in dispersed capacity, yet the other mixed records outside the set stay arranged.

4 .Conclusion

The venture proposed an adaptable security saving information sharing (FPDS) plot in cloud-helped IoT. The FPDS conspire is described by utilizing personality based encryption and straight mystery sharing plan to not just save the protection of information moved to the cloud yet additionally accomplish adaptable sharing of scrambled information. Point by point security investigation shows that the FPDS conspire is secure against semi-confided in cloud and malevolent clients. Careful execution assessment shows the high proficiency of the plan. The FPDS conspire permits to scramble information with any unmistakable personality and in this manner evades muddled public-key authentications in normal secure stockpiling frameworks. Also to the character based encryption, notwithstanding, the FPDS conspire just permits to share information to one beneficiary, which makes it hard to impart information to a gathering of clients. In our future work, we might check for more broad arrangements on premise of transmission/characteristic based encryption, to help security saving information sharing for various beneficiaries in cloud-helped IoT situations.

References

C. Wang, N. Cao, J. Li, K. Ren, W. Lou. “Secure ranked keyword search over encrypted cloud data”[C]//IEEE 30th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2010: 253-262.

Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Deen. “Privacy-preserving Double-Projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning,” IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.

R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, “Dual-Server PublicKey Encryption with Keyword Search for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 789-798.

X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. ”An efficient privacypreserving outsourced calculation toolkit with multiple keys.” IEEE Transactions on Information Forensics and Security 11.11 (2016): 2401-2414.

B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, 2004.

Murugesan, M., Thilagamani, S. ,” Efficient anomaly detection in surveillance videos based on multi layer perception recurrent neural network”, Journal of Microprocessors and Microsystems, Volume 79, Issue November 2020, https://doi.org/10.1016/j.micpro.2020.103303.

W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, “Protecting Your Right: Verifiable Attribute-based Keyword Search with Finegrained Owner-enforced Search Authorization in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

K. Liang, W. Susilo, “Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 19811992.

Thilagamani, S., Nandhakumar, C. .” Implementing green revolution for organic plant forming using KNN-classification technique”, International Journal of Advanced Science and Technology, Volume 29 , Isuue 7S, pp. 1707–1712

J. Lai, R. H. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Transactions o Information Forensics and Security, 2013, vol. 8, no. 8, pp. 13431354.

B. Qin, R. H. Deng, S. Liu, and S. Ma, “Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1384-1394.

Thilagamani, S., Shanti, N.,” Gaussian and gabor filter approach for object segmentation”, Journal of Computing and Information Science in Engineering, 2014, 14(2), 021006, https://doi.org/10.1115/1.4026458

Z. Liu, Z. Cao, D.S. Wong, “White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures,” IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 1, pp. 76-88.

Rhagini, A., Thilagamani, S. ,”Women defence system for detecting interpersonal crimes”,International Journal of Advanced Science and Technology, 2020, Volume 29,Issue7S, pp. 1669–1675

Z. Liu, Z. Cao, D.S. Wong, “Traceable CP-ABE: how to trace decryption devices found in the wild,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.

K.Deepa, S.Thilagamani, “Segmentation Techniques for Overlapped Latent Fingerprint Matching”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-12, October 2019. DOI: 10.35940/ijitee.L2863.1081219

P. Xu, H. Jin, Q. Wu and W. Wang, “Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gusssing Attack,” IEEE Transactions on Computers, 2013, vol. 62, no. 11, 2266-2277.

Q. Tang, “Nothing is for Free: Security in Searching Shared and Encrypted Data,” IEEE Transactions on Information Forensics and Security, 2014, vol. 9, no. 11, 1943-1952.

Kumararaja, V., Deepa, K.,” Pap smear image classification to predict urinary cancer using artificial neural networks” , Annals of the Romanian Society for Cell Biology, ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1092 – 1098

B. Zhang, F. Zhang, “An efficient public key encryption with conjunctive-subset keywords search,” Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 262-267.

Santhi, P., Mahalakshmi, G., Classification of magnetic resonance images using eight directions gray level co-occurrence matrix (8dglcm) based feature extraction, International Journal of Engineering and Advanced Technology, 2019, 8(4), pp. 839–846.

J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2nd ed. CRC Press, 2014.

D. Song, D. Wagner, and A. Perrig, “Practical Techniques for Searches on Encrypted Data,” in Proc. of IEEE S&P’00, 2000.

Santhi, P., Lavanya, S., Prediction of diabetes using neural networks, International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1160–1168

R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,” in Proc. of ACM CCS’06, 2006.

Pandiaraja, P, Vijayakumar, P, Vijayakumar, V & Seshadhri, R 2017, ‘Computation Efficient Attribute Based Broadcast Group Key Management for Secure Document Access in Public Cloud’, Journal of Information Science and Engineering, 33, No. 3, pp. 695-712.

S. Kamara and C. Papamanthou, “Parallel and Dynamic Searchable Symmetric Encryption,” in Proc. of FC, 2013.

D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, “Highly-Scalable Searchable Symmetric En- cryption with Support for Boolean Queries,” in Proc. of CRYPTO’13, 2013.

D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, “Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation,” in Proc. of NDSS’14, 2014.

Vijayakumar, P ,Pandiaraja, P, , Karuppiah, M & Deborah, LJ 2017, ‘An Efficient Secure Communication for Healthcare System using Wearable Devices’, Journal of Computers and Electrical Engineering, Elsevier , Vol .No 63 , October 2017 , pp 232-245

Vijayakumar, P, Pandiaraja, P, Balamurugan, B & Karuppiah, M 2019, ‘A Novel Performance enhancing Task Scheduling Algorithm for Cloud based E-Health Environment’, International Journal of E-Health and Medical Communications (IJEHMC), Vol 10,Issue 2,pp 102-117.

R. Cheng, J. Yan, C. Guan, F. Zhang, and K. Ren, “Verifiable Searchable Symmetric Encryption from Indistinguishability Obfuscation,” in Proc. of ACM AISACCS’15, 2015.

P. Pandiaraja, N Deepa 2019 ,” A Novel Data Privacy-Preserving Protocol for Multi-data Users by using genetic algorithm” , Journal of Soft Computing , Springer , Volume 23 ,Issue 18, Pages 8539-8553

J. Benaloh and M. de Mare, “One-way Accumulators: A Decentralized Alternative to Disgital Signatures,” in Proc. of EUROCRYP’93, 1993.

N Deepa , P. Pandiaraja, 2020 ,” Hybrid Context Aware Recommendation System for E-Health Care by merkle hash tree from cloud using evolutionary algorithm” , Journal of Soft Computing , Springer , Volume 24 ,Issue 10, Pages 7149–7161.

J. Katz and Y. Lindell, "Aggregate Message Authentication Codes," in Proc. of CT-RSA'08, 2008.

N Deepa , P. Pandiaraja, 2020 , " E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption ", Journal of Ambient Intelligence and Humanized Computing , Springer , https://doi.org/10.1007/s12652-020-01911-5

B. Wang and X. Fan, "Lightweight Verification for Searchable Encryption," University of Cincinnati, Tech. Rep., 2018. [Online]. Available: http://homepages.uc.edu/~wang2ba/

L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

K Sumathi, P Pandiaraja 2019," Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks" , Journal of Peer-to-Peer Networking and Applications , Springer , Volume 13,Issue 6,Pages 2001-2010.

Wenzhong Guo, Jie Li, Senior Member, Guolong Chen, Yuzhen Niu,and Chengyu Chen, "A PSO-optimized Real-time Fault-tolerant Task Allocation Algorithm in Wireless Sensor Networks"

Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, Man Ho Au " Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption"

Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., Sharma, P. ," Privacy preserving E-voting cloud system based on ID based encryption " Journal of Peer-to-Peer Networking and Applications , Springer , https://doi.org/10.1007/s12083-020-00977-4..

C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.