Efficient Management that Enables Diverse Access to Secure Internet of Things Fog-Based Data

E. Sai Kumar[1], Dr. C.V. Madhusudan Reddy[2], Dr. K. Venkataramana[3], M. Akshitha Laasya[4], B. Naga Raju[5]

[1,2,3,5] Department of Computer Science and Engineering
[4]Department of Information of Technology
[1,2, 3, 5] QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India
[4]CVR College of Engineering
[1]saikumar.e@qiscet.edu.in, [2]madhusudanreddy.c@qiscet.edu.in, venkataramana.k@qiscet.edu.in
[4]20B81A1206@cvr.ac.in,[5] nagaraju.b@qiscet.edu.in
Corresponding Author Mail: qispublications@qiscet.edu.in

Article Info
Page Number: 226-235
Publication Issue:
Vol. 69 No. 1 (2020)

Article History
Article Received:
12 September 2020
Revised: 16 October 2020
Accepted: 20 November 2020
Publication: 25 December 2020

Abstract

To maintain data privacy and control who has access to what in the cloud, attribute-based encryption might be utilized. Attribute security is violated when apparent qualities are introduced to the encrypted message to assist people identify necessary details in vast systems. To offer an effective attribute-based access control with an authorized search strategy, this research expands the anonymous key-policy attribute-based encryption (AKP-ABE) to provide fine-grained data retrieval while safeguarding attribute privacy (EACAS). In EACAS, data users may generate the trapdoor using the secret key supplied by data owners and conduct searches based on access restrictions to get the relevant data. Cryptographic protocols and trapdoor generation use a synthetic property devoid of syntactic significance to provide an attribute-based searching on the exported encoded information in the fog. Data owners may implement granular access control on their outsourced data by establishing the search criteria that will be used by data consumers to locate relevant content based on protected attributes. We show that compared to the state-of-the-art methods, EACAS requires less time and space to process and store data.

Keywords: Access control, authorized search, cloud storage, data sharing, key-policy attribute-basedencryption.

I. INTRODUCTION

IoT device data may be sent to the fog for storage and analysis via a number of IoT management services, such as Amazon AWS IoT [1] and Google Cloud IoT Core [2]. In cloud-based management systems, asymmetrical and complex trust linkages between IoT devices from several trust domains are typical. As a result, it could be difficult to control access to what in the outsourcing IoT data from an unified security perspective. Attribute-based encryption (ABE) is one solution since it provides rules-based, granular access control to encrypted data in a safe manner [3]. In ciphertext-policy ABE (CP-ABE) [4, the encryptor is able to specify the ciphertext's access policy using a collection of descriptors. Even if an attacker obtains a decryption key.

Cloud-based management of the Internet of Things (IoT) requires the resolution of various issues before CP-ABE may be utilised for this purpose. More characteristics initially cause the ciphertext to grow in size [5, 6, 7]. This might be a significant challenge for IoT systems due to the vast range of capabilities needed for IoT applications and services [8]. CPABE approaches, which only permit ciphertexts of fixed size [9, 10, 11, 12], are insufficient to ensure the security of IoT systems.

CP-main ABE's benefit is that it may be used on battery-powered mobile devices like laptops since the majority of the computational work is placed on the decryptor (rather than the encryptor). Recent studies have shown that an unauthorised cloud provider may decode a user's communication. Because of this, the cipher-text amount was unreadable. Decryption that can be outsourced [5] and cypher text of fixed size Advanced Behavioral Economics (ABE) techniques are only two examples of state-of-the-art technologies that might be combined to address these issues. The problem cannot be fixed using the outsourced decoding approach [5] due to the use of a key blindness methodology. The cloud may return partly decrypted data disguised by z if sensitive information is veiled using a (secret) blinding factor, such as z, and then sent back to the user. Because of this, finding it just requires z. However, this method includes extra material critical to decryption that is concealed from the user in continuously encrypted text [11]. The user can never be certain they have successfully retrieved the plaintext as a result.

A technique to concurrently create compact secure messages and subcontractable decryption was developed by Li et al. [16]. However, decoding a cipher text is only possible for users for whom traits match those in the access policy, which severely limits the ability to govern access. Finally, if users give their private keys to people who are not authorised to do so, there is a risk of improper usage of secret keys. As a result, both authorised and unauthorised users may engage in inappropriate exchanges of secret keys. Anybody with an internet connection might potentially get access to the data gathered by IoT gadgets. Using ABE that could be traced has been suggested to the leakage problem in past research. The primary limitation of most key-tracing algorithms is that they only seek for the original key-holders. If that's the case, dishonest individuals may still access your cloud data by giving out their private keys. Key leaking cannot be prevented only through traceability since there are practical methods for recovering keys, such as session hijacking analysis. They may still access and recover the information up until the key expires, this is not a workable solution to the shared (or leaked) key problem. An efficient system for Authentication that represents existing issues is crucial for fog IoT management solutions. A safe and efficient IoT data management system that functions in the cloud's fog environment is made possible by our innovative CPABE architecture. If implemented, the proposed method may efficiently manage storage and capacity while also tracking down and punishing saboteurs who disseminate their private keys in a dishonest manner. By providing the cloud with a client transformation key, It might be able to outsource the majority of the decryption-related computation. To prevent unauthorized brought on public digital key, the Fog authorized the digital key, decrypts the encrypted message partially using the transformation key of the digital key, and then returns the partially decoded output. Remember that the attribute key and the transformation key are closely coupled, and that only the original owner of the attribute key has the ability to decrypt the partly encrypted text and return normal. No one else can decode the message using the public keys. As opposed to summarising, the recommended method may survive assaults like key misuse that are challenging to meticulously decipher.

II. RELATEDWORKS

These issues may be remedied by using constant-size ciphertext [11] and outsourceable decryption [5] in ABE systems. However, the outsourced decryption approach [5] does not work because of a key blinding mechanism. Using a (secret) blinding factor called z, the user may obscure their own private key from prying eyes. As a result, the cloud may do a blindfolded key decryption and provide the original, unmasked plaintext. Because of this, finding it just requires z. However, when using this technique, not only is z concealed from the user, but so are other crucial parts of the constant-size ciphertext [11]. Because of this, the user can no longer extract the plaintext with any degree of certainty. Li et al. [16] developed a method to accomplish both a compact ciphertext and a decipherment that may be subcontracted.

Data from IoT sensors may be routed to either centralised or decentralised cloud servers for storage, transit, and processing, making these systems vulnerable to both internal and external assaults. The proliferation of IoT has been greatly aided by cloud computing's vast capacity for data storage and processing. To protect IoT data from hackers and other bad actors, many encryption methods have been put into place. Mathematics on encrypted data is a challenging task. Full-homomorphy encryption might be implemented using a semi-trusted server. It's challenging to design a distributed system for exchanging data across IoT devices. To solve this problem, a completely homomorphic encryption system tailored to cloud-based IoT applications was designed. Semi-trusted servers allow homomorphic multiplications to be calculated without first decrypting the input. The term "e-Health" is used to refer to a healthcare infrastructure that is based on the use of the Internet and other networked infrastructure. For this analysis, we looked at how the usage of intelligent technologies in healthcare has evolved from 2017 to 2020, specifically focusing on how cloud computing and IoT devices have affected this trend. E-health refers to the collection and analysis of health information from electronic sources with the purpose of improving patient care in terms of diagnosis, treatment, and prevention. The Internet can protect consumers and encourage them to take an active part in their own health care decision-making via the centralization of medical data and e-Health research. Low rates of e-Health adoption increase the likelihood that individuals may encounter bogus claims. The potential, benefits, and challenges of establishing IoT-cloud-based health systems are assessed from a number of different viewpoints. Intelligence-driven goal-finding and innovative application-development have led to some exciting new combinations in the Internet of Things, cloud computing, and eHealth systems. The Internet of Things raises a variety of concerns about the protection of private information and sensitive data. Challenges facing the Internet of Things include insufficient security measures, user illiteracy, and ubiquitous active device monitoring. As we examine the past of IoT systems and security measures, we can learn more about (a) different types of security and privacy worries, (b) current security solutions, and (d) the best privacy models required and suitable for different tiers of IoT-driven applications. In this research, we laid out the layered structure of the IoT and identified its numerous parts, from the most fundamental to the most complex safeguards for user data. The proposed cloud/edge system for the Internet of Things has been implemented and validated.

Internet of Things nodes are supported by Amazon Web Services (AWS) Virtual Machines. The Raspberry Pi 4 hardware kit hosted by Amazon Web Services was used to build the intermediate layer of the Greengrass Edge Environment (edge). Our approach is built on top of the Amazon Web Services (AWS) IoT cloud infrastructure (the cloud). The management sessions and other security measures ensured that user data remained secure at all times. We built security certificates to allow for encrypted communication between the different nodes in the proposed cloud/edge enabled IoT architecture. Threats to the security of the cloud, edge, and IoT layers might be mitigated by adopting the suggested system architecture and using current best practises in information security. It's safe to say that the combination of CC and the IoT has had a major impact on contemporary medical practise (IoT). Due to the increasing data output from IoT devices, a centralised data storage and processing infrastructure such as the CC is becoming more important. As more people and IoT devices depend on remote access to computer and networking resources, the need for security in CoT is increasing.

This is a very crucial case for preserving people's right to internet anonymity. That the CoT is giving security and privacy more attention is clear from this. In this article, we looked at the problems and possible answers around data security and privacy. Research on the CoT's underlying architecture and its present uses has been undertaken toward this end. Challenges and impediments that have still to be addressed, as well as other concerns connected to privacy and security, are also explored.

III. PROPOSED SYSTEM ARCHITECTURE

We offer a secure and effective solution for handling IoT data in the cloud using our state-of-the-art CPABE architecture. The proposed method may identify traitors who unintentionally release private keys while also efficiently controlling memory and bandwidth. Cloud services may be able to outsource a large portion of the computation needed for decryption if they provide each user their own unique transformation key.

In order to avoid unapproved shared by receipient who has been compromised, the fog verifies the identification of the key holder, decodes some of the encrypted message by employing receipents transition, and returns the result. You should be aware that the original owner of an attribute key is actively taking part in the process since only he is capable of decrypting plaintext. The plaintext cannot be used while using the shared (or compromised) keys. The owner of the data first has to create an account on a remote server and authorise access. The file will be encrypted and uploaded to the cloud server when the owner receives permission from the cloud data owner. The owner will then request the information key and secret for the file he submitted. To do deduplication in the cloud, the file must first be produced using unique keys. Users may only view, download, and otherwise interact with submitted files if the data's owner has granted them access. The cloud storage service is run and maintained by a cloud server. Files containing sensitive information are encrypted before being uploaded to the cloud, where approved End users may view, edit, and interact in real time. Users will require both the content key and the master secret key to access the joint data files. The cloud will also maintain track of all connected transactions and attacks, in addition to easing access. Key Authority is contacted by the customer when they need a secret key and content key. KeyAuthority can see any file and retrieve its associated content key, master secret key, and data owner details. Cloud-based information is inaccessible without a user account and associated credentials.

The person's account has been given access by the cloud, which will now confirm their registration. The private key and the Information key must first be requested by the user prior to being able to view the file. Users are free to search and download files as registered owner permits it.

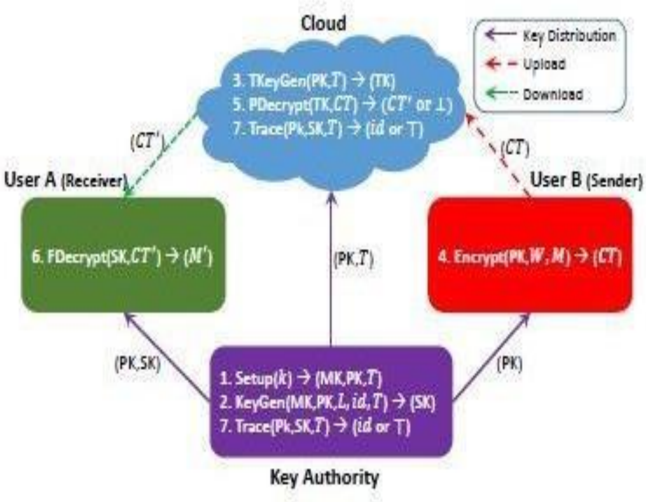

Fig:1Methodology used

IV. RESULTS AND DISCUSSION

The acquired findings are displayed in Figs. 2 through 5..

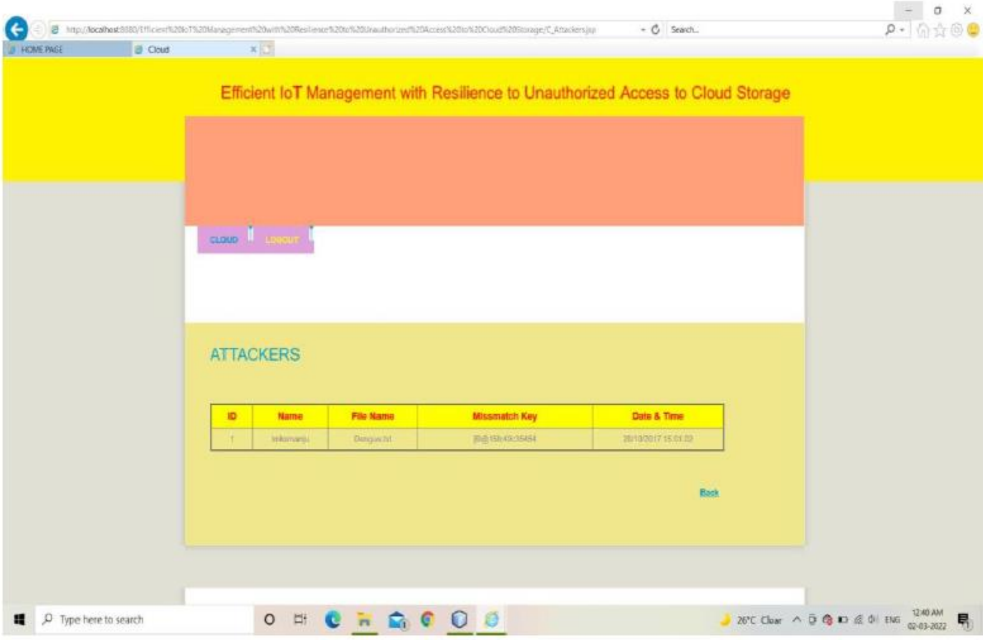

Fig.2 Hacker

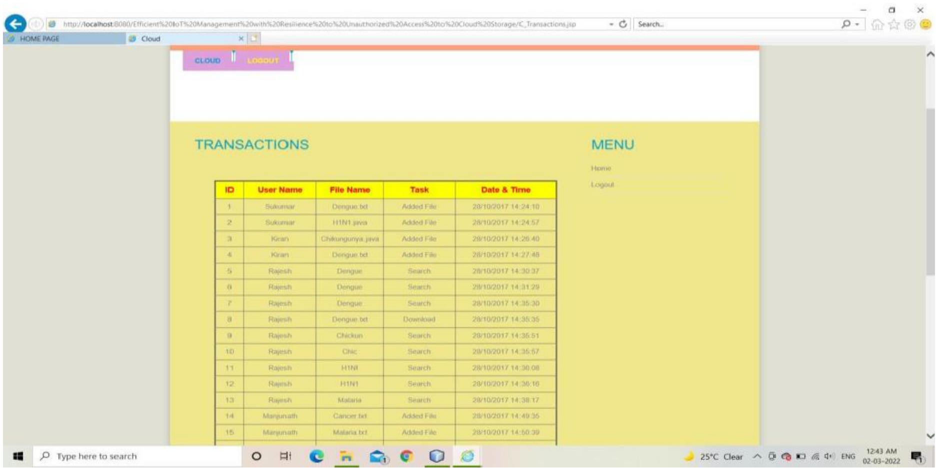

Fig 3.Proceedings

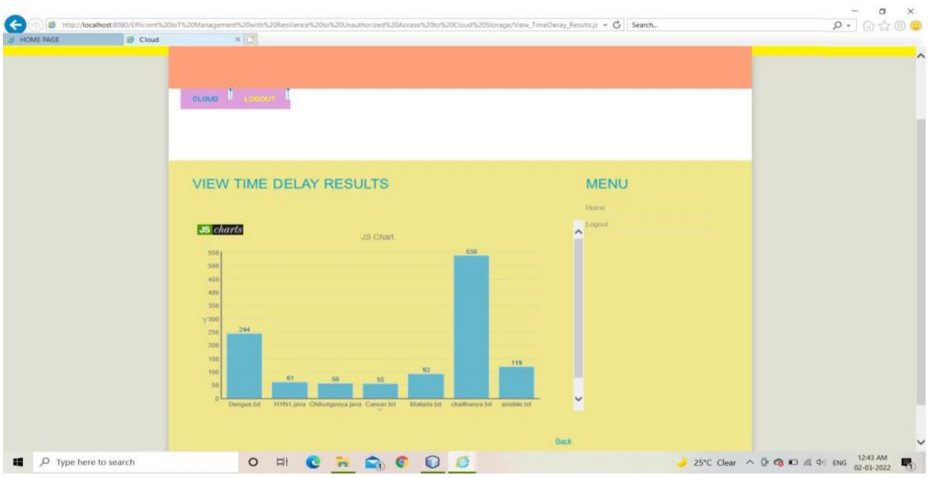

Fig.4Examine the Time Delay outcomes

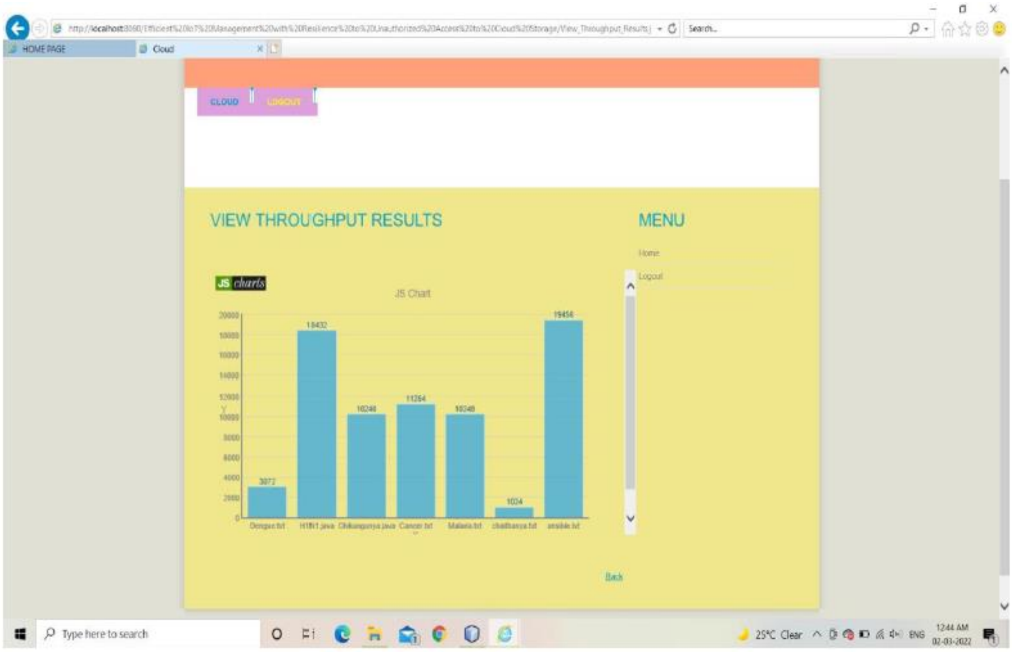

Fig.5 Look at the Output Data

V. FUTURE SCOPE AND CONCLUSION

Alternatives for fog The innovative CP-ABE technique may be useful for Internet administration. The recommended approach saves money on communication expenses since Sensor nodes produce an encrypted message of a fixed size regardless of the quantity of characteristics. Under the proposed method, user devices running on battery power might offload most of the decryption work to the cloud. By tracing back where a key came from, you can be sure that only the key's rightful owner may decrypt an encrypted file, protecting it from those who may have gained access to it illegally. Attacks using forensically intractable key misuse are widespread in IoT systems, but the proposed method is resilient to them.

REFERENCES

[1] “AWS IoT.” AWS. https://aws.amazon.com/ko/iot. (accessed Dec. 17, 2019)
[2] “Cloud IoT Core.” Google Cloud. https://cloud.google.com/iotcore. (accessedDec. 17, 2019)
[3] A. Sahai, B. Waters, “Fuzzy identity-based encryption,” Advances in Cryptology-EUROCRYPT, 2005, pp. 457–473.
[4] J. Bettencourt, A. Sahai, B. Waters, “Ciphertext-policy attributebasedencryption,” In IEEE symposium on security and privacy (SP’07), 2007, pp. 321–334.
[5] M. Green, S. Hohenberger, B. Waters, “Outsourcing the decryption of ABEciphertexts,” In USENIX Security Symposium, Vol. 2011, No. 3, 2001.
[6] J. Lai, R. H. Deng, C. Guan, J. Weng, “Attribute-based encryption with verifiableoutsourced decryption,” IEEE Transactions on Information Forensics and Security,8(8), 2013, pp. 1343–1354.

[7] S. Lin, R. Zhang, H. Ma, M. Wang, "Revisiting attribute-based encryption withverifiable outsourced decryption," IEEE Transactions on Information Forensics andSecurity, 10(10), 2015, pp. 2119–2130.
[8] S. Sours, I. P. Barco, P. Zwickl, I. Gojmerac, G. Bianchi, G. ˇ Carrozzo,"Towards the cross-domain interoperability of IoT platforms," In EuropeanConference on Networks and Communications (EuCNC), 2016, pp. 398–402.
[9] C. Chen, Z. Zhang, D. Feng, "Efficient ciphertext policy attributebasedencryptionwith constant-size ciphertext and constant computation-cost," In Provable Security,2011, pp. 84–101.
[10] C. Hahn, H. Kwon, J. Hur, "Efficient attribute-based secure data sharing withhidden policies and traceability in mobile health networks," Mobile InformationSystems, 2016.
[11] Z. Zhou, D. Huang, Z. Wang, "Efficient privacy-preserving ciphertext-policyattribute based-encryption and broadcast encryption," IEEE Transactions onComputers, 64(1), 2015, pp. 126–138.
[12] Z. Zhou, D. Huang, "On efficient ciphertext-policy attribute based encryptionand broadcast encryption," In Proceedings of the 17th ACM conference on Computerand communications security, 2010, pp. 753–755.
[13] Shang, W., Bann's, A., Liang, T., Wang, Z., Yu, Y., Afanasyev, A., and Zhang,L., "Named data networking of things," In IEEE First International Conference onInternet-of-Things Design and Implementation (IoTDI), 2016, pp. 117–128.
[14] Gibb, J., Buyya, R., Maurice, S., and Palaniswami, M., "Internet of Things (IoT): A vision, architectural elements, and future directions," Future generationcomputer systems, 29(7), 2013, pp. 1645–1660.
[15] Ghose, A., Biswas, P., Bhaumik, C., Sharma, M., Pal, A., and Jha, A., "Roadcondition monitoring and alert application: Using invehicle smartphone as internet -connected sensor," In IEEE International Conference on Pervasive Computing andCommunications Workshops (PERCOM Workshops), 2012, pp. 489–491.
[16] Li, J., Sha, F., Zhang, Y., Huang, X., and Shen, J., "Verifiable outsourceddecryption of attribute-based encryption with constant ciphertext length," Securityand Communication Networks, 2017.
[17] Y. Jiang, W. Susilo, Y. Mu, F. Guo, "Ciphertext-policy attributebasedencryptionagainst key-delegation abuse in fog computing," Future Generation ComputerSystems,78, 2017, pp. 720–729.
[18] Y. B. Saied, A. Livereaf, D. Zeghlache, M. Laurent, "Lightweight collaborativekey establishment scheme for the Internet of Things," Computer Networks, 64, 2014,pp. 273–295.
[19] M. J. Hinek, S. Jiang, R. Safavi-Naini, S. F. Shahandashti, "Attribute-basedencryption with key cloning protection," International Journal of AppliedCryptography, 2(3), 2012, pp. 250–270.
[20] S. Yu, K. Ren, W. Lou, J. Li, "Defending against key abuse attacks in KP –ABEenabled broadcast systems," In International Conference on Security and Privacy inCommunication Systems, 2009, pp. 311–329.

[21] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, D. Xie, "Multi-authorityciphertext-policy attribute-based encryption with accountability," In Proceedings ofthe 6th ACM Symposium on Information, Computer and Communications Security,2011, pp. 386–390.

[22] Z. Liu, Z. Cao, D. S. Wong, "Blackbox traceable CP-ABE: how to catch peopleleaking their keys by selling decryption devices on ebay," In Proceedings of the ACMSIGSAC conference on Computer & communications security, 2013, pp. 475–486.

[23] J. Ning, Z. Cao, X. Dong, L. Wei, X. Lin, "Large universe ciphertext–policyattribute-based encryption with white-box traceability," In European Symposium onResearch in Computer Security, 2014, pp. 55–72.

[24] G. Yu, Z. Cao, G. Zeng, W. Han, "Accountable ciphertext-policy attribute-basedencryption scheme supporting public verifiability and nonrepudiation," InInternational Conference on Provable Security, 2016, pp. 3–18.

[25] J. King, Z. Cao, X. Dong, J. Gong, J. Chen, "Traceable CP -ABE with shortciphertexts: how to catch people selling decryption devices on eBay efficiently," InEuropean Symposium on Research in Computer Security, 2016, pp. 551–569.

[26] P Ramprakash, M Sakthivadivel, N Krishnaraj, J Ramprasath. "Host-based Intrusion Detection System using Sequence of System Calls" International Journal of Engineering and Management Research, Vandana Publications, Volume 4, Issue 2, 241-247, 2014

[27] N Krishnaraj, S Smys."A multihoming ACO-MDV routing for maximum power efficiency in an IoT environment" Wireless Personal Communications 109 (1), 243-256, 2019.

[28] N Krishnaraj, R Bhuvanesh Kumar, D Rajeshwar, T Sanjay Kumar, Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor networks, 2020 International Conference on Inventive Computation Technologies (ICICT),201-204

[29] Ibrahim, S. Jafar Ali, and M. Thangamani. "Enhanced singular value decomposition for prediction of drugs and diseases with hepatocellular carcinoma based on multi-source bat algorithm based random walk." Measurement 141 (2019): 176-183. https://doi.org/10.1016/j.measurement.2019.02.056

[30] Ibrahim, Jafar Ali S., S. Rajasekar, Varsha, M. Karunakaran, K. Kasirajan, Kalyan NS Chakravarthy, V. Kumar, and K. J. Kaur. "Recent advances in performance and effect of Zr doping with ZnO thin film sensor in ammonia vapour sensing." GLOBAL NEST JOURNAL 23, no. 4 (2021): 526-531. https://doi.org/10.30955/gnj.004020 , https://journal.gnest.org/publication/gnest_04020

[31] N.S. Kalyan Chakravarthy, B. Karthikeyan, K. Alhaf Malik, D.Bujji Babbu,. K. Nithya S.Jafar Ali Ibrahim , Survey of Cooperative Routing Algorithms in Wireless Sensor Networks, Journal of Annals of the Romanian Society for Cell Biology ,5316-5320, 2021

[32] Rajmohan, G, Chinnappan, CV, John William, AD, Chandrakrishan Balakrishnan, S, Anand Muthu, B, Manogaran, G. Revamping land coverage analysis using aerial satellite image mapping. Trans Emerging Tel Tech. 2021; 32:e3927. https://doi.org/10.1002/ett.3927

[33] Vignesh, C.C., Sivaparthipan, C.B., Daniel, J.A. et al. Adjacent Node based Energetic Association Factor Routing Protocol in Wireless Sensor Networks. Wireless Pers Commun 119, 3255–3270 (2021). https://doi.org/10.1007/s11277-021-08397-0.

[34] C Chandru Vignesh, S Karthik, Predicting the position of adjacent nodes with QoS in mobile ad hoc networks, Journal of Multimedia Tools and Applications, Springer US,Vol 79, 8445-8457,2020