International Journal of System Design and Computing
Volume 02, Issue 01, January – June (2024)

RESEARCH ARTICLE

DNA ENCRYPTION-BASED SECURE ACCESS CONTROL AND DATA SHARING IN AN ENABLED CLOUD ENVIRONMENT

A.R. Aarthy [1, *] and K. Vinoth Kanth [2]

[1] Department of Computer Science and Engineering, Satyam College of Engineering and Technology, Aralvaimozhi, Anna University, India.
[2] Department of Computer Science and Engineering, University college of engineering Nagercoil, India.

[*]*Corresponding e-mail: aarthyvishnu343@gmail.com*

Abstract – IoT and cloud service providers are vulnerable to both internal and external threats consequently it is not possible to fully trust them with sensitive customer data. The cloud should offer a mechanism for the user to verify if the integrity of his data is being maintained or if it has been compromised, as the user cannot physically judge the data. Cloud computing is the best solution for storing this type of data. IoT has introduced secure data sharing and access management to prevent this issue. However, centralized access control presents a number of difficulties. The goal is to develop a novel DNA Encryption-based Secure Access Control and Sharing (DESACS) technique that has been proposed in an IoT-enabled Cloud environment which enhances the privacy and security of IoT data. The privacy of IoT has been increased by encrypting the data using the DNA cryptography (DNAC) encryption technique. It offers fresh hope for breaking invincible algorithms. This is a result of DNA computing's increased speed, low storage needs, and power consumption. In contrast to traditional storage media, which require 1012 nm3/bit, DNA stores memory at a density of roughly 1 bit/nm3.

Keywords – *Internet of Things, DNA, Cloud, DNA Encryption*.

1. INTRODUCTION

The development of Internet of Things (IoT) technology has made it possible for several things to communicate with one another, opening up a variety of applications such as smart manufacturing, smart transportation, and smart housing [1]. Sharing data has become a standard practice for individuals, scientific groups, educational institutions, and the medical business. IoT has seen a sharp rise in demand, acceptance, and commercial availability in the last few years [2]. The IoT is vulnerable to the leakage of private information during data exchange. Medical data is critical to patient care, research, and public health. It provides critical information to healthcare professionals, allowing them to make informed decisions about diagnosis and treatment, while also funding research efforts to better understand diseases, develop new therapies, and improve patient outcomes [3]. Data exchange both inside and outside of organizations is essential for industries and financial institutions [4]. A wide network with a number of IoT-enabled apps and devices makes up the cloud architecture based on the Internet of Things [5].

Cloud computing is the process of delivering computation and resources over the internet as a service rather than a product, enabling users to access databases, information, hardware, software, and other resources anytime they're needed [6]. Consumers utilize on-demand services and pay for them without taking into account the initial expenses of infrastructure and ongoing maintenance [7]. Cloud computing has gained significant attention recently and is growing in popularity as a result of these benefits [8]. These days, there are numerous cloud service providers, including Microsoft Azure, Amazon EC2, and others [9]. Considering their vulnerability to both internal and outsider assaults, cloud and IoT service companies cannot be completely trusted with sensitive personal data [10]. The cloud should offer a way for the user to ascertain whether the integrity of his data is preserved or jeopardized because the data is not physically available to consumers [11]. Cloud computing is the best way to store this type of data. One major problem is the lack of interoperability between different IoT devices and apps on the cloud design. To address this issue, a novel DNA Encryption-based Secure Access Control and Sharing (DESACS) technique that has been proposed in an IoT-enabled Cloud environment which enhances the privacy and security of IoT data.

2. LITERATURE REVIEW

In 2020 Rashid, et al. [12] proposed the implementation of Internet of Things medical data stored on public cloud platforms in healthcare systems is secured using Enhanced Role Based Access Control (ERBAC). A secure cloud system for storing medical data based on role-based access policies will be made possible by the suggested system it will also significantly aid in the efficient storage of medical data from online applications. This model provides the required

limitations on responsibilities and uses to guarantee the safety of health information kept on cloud-based platforms.

In 2021 Shi, et al. [13] proposed DUCE, a distributed employ control enforcement approach for CEIoT data exchange. The suggested approach makes use of Trusted Execution Environment (TEE) and blockchain technology to provide dependable and continuous enforcement of the cross-domain data-sharing lifecycle. Comparing the findings to OAuth 2.0, the performance and scalability overhead are tolerable. An open-source permissioned blockchain system prototype is being evaluated through the experimental deployment.

In 2022 Kitagawa, et al. [14] proposed SINETStream a method for sharing and safely encrypting data using a Secure Configuration Server. Confidential information is given to recipients through the mechanism in an encrypted manner restricting access to only those that are permitted. This approach makes it simple to share sensitive data since it securely manages data encryption keys within the system, something that traditional systems have made difficult.

In 2023 Fugkeaw, et al. [15] developed LightMED, an access control system that combines blockchain, CP-ABE, and fog computing to enable safe, scalable, and fine-grained EMR sharing in a cloud-based environment. It conducted trials to evaluate our plan's and related works' efficacy and finished a comparative analysis to illustrate the computation cost. The design suggests a mechanism for securely transmitting and aggregating IoT data that is based on digital signing and lightweight encryption. The method's principal addition includes an access policy mechanism that protects privacy along with outsourced encryption.

In 2023 Liu, et al. [16] proposed BP-AKAA, a attribute-based access control made possible by a key agreement method and cross-domain private-protected authentication implemented by blockchain technology. Device identities are safeguarded by the use of non-interactive zero-knowledge proof technology. Performance investigation indicates that this method outperforms current approaches in terms of access control, authentication, and key generation. It also fulfills a number of requirements including as mutual authentication, privacy preservation, and cross-domain functionality.

In 2023 Han, et al. [17] introduced a blockchain-based, internal product encryption-based Internet of Things access management method. Inner product encryption provides fine-grained access control, complete concealment of access limitations, and data security and user privacy for lightweight Iot devices by utilizing the property of vector representation of characteristics. The mechanism can match the specific access control requirements of the Internet of Things and has great efficiency while guaranteeing security, according to the experimental findings.

In 2024 Singh, et al. [18] proposed the DNACDS access control model and cryptography technique to solve the massive data security and access issues in the Internet of Everything. Deoxyribonucleic acid (DNA) computing is a biological idea that potentially enhances Internet of Everything (IoE) large data security. The suggested method outperforms other DNA-based security systems, as demonstrated by the experimental results. Better resistance capabilities are revealed by the DNACDS's theoretical security research.

3. PROPOSED METHOD

In this section a novel DNA Encryption-based Secure Access Control and Sharing (DESACS) technique that has been proposed in an IoT-enabled Cloud environment which enhances the privacy and security of IoT data. The privacy of IoT has been increased by encrypting the data using the DNA cryptography (DNAC) encryption technique (Figure 1).

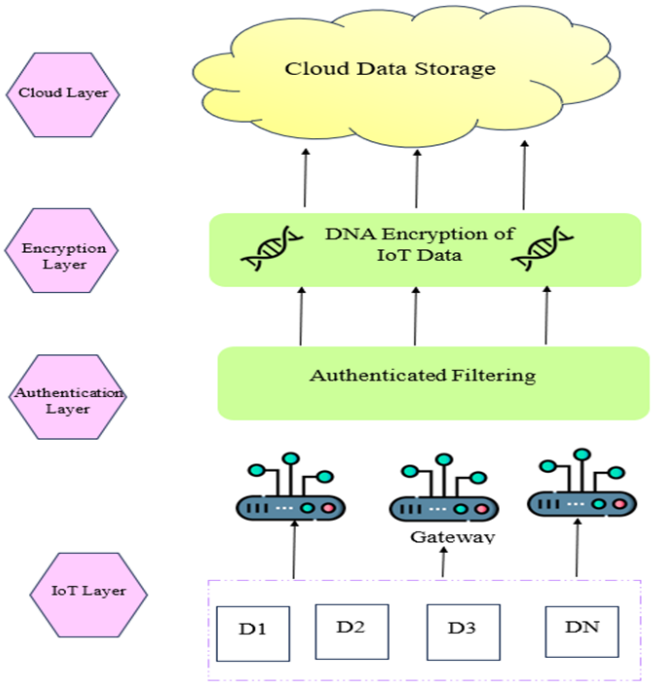

Figure 1. Block diagram of proposed DESACS technique

3.1. IoT Layer

The IoT layer represents the foundation of the system where various Internet of Things (IoT) devices, labelled from D1 to DN, are interconnected. The data collection and transmission to the gateways is the responsibility of these devices from their respective contexts. The depiction of multiple devices suggests a scalable network capable of handling a range of IoT devices, each potentially monitoring different parameters or performing distinct functions. This layer is crucial as it serves as the data source for the subsequent security and storage processes in the system's architecture.

3.2. Authentication Layer

The authentication layer serves as the gatekeeper to a system, verifying the identity of users and granting access to authorized individuals or entities. This layer guards against unauthorized access and potential security risks while guaranteeing that only authorized users are given access to the system's resources and services.

3.2.1. Authentication-Based Request Filtration

Through the GW, users can submit a request message to the EN for real-time access to the IoT devices. Request filtration is carried out by the GW to lessen DDoS assaults brought on by unauthorized user requests. First, the GW uses filters to confirm the legitimacy of the users that created the requests. The filter initially begins with an m-bit empty array. When the element's eligibility for the filter is confirmed, it returns false. The element must first be approved by the hash function in order to be added to the filter. In this instance, hashing is done using the SHA-256 technique. The result of the hash function is used to determine a location in the filter's array. One is assigned to the bit's location. The places in the filter are created using hash functions, which are then used to check the element in the filter. The filter indicates that the request is valid if every position in the array is one; if not, it is invalid. Therefore, to validate the elements in the array, the hash function is employed. Furthermore, it serves to confirm the request's validity. The definition of the filter's false positive rate (σ) for large values of m is as follows:

$$\sigma = (1 - a^{-\frac{ep}{k}})^e \quad (1)$$

where e and p stand for the false positive rate, e for the nearest power 2 value, and p is rounded to the closest integer value. The number of elements in the filter is indicated by Q. It only filters valid requests based on the filter. The timestamp and freshness of the arriving packets are checked to make sure the user is authentic. This will screen and ignore the unauthorized access requests that are triggering denial-of-service attacks. The load on access delegation is lessened because only valid access requests are handled.

3.3. Encryption Layer

The encryption layer serves as a crucial component of security infrastructure, safeguarding data by converting it into an unreadable format using cryptographic algorithms. This layer ensures the confidentiality and integrity of information transmitted or stored within a system by encoding data into ciphertext, meaning that only people with the right authorization and decryption keys may decode it. This uses DNA encryption to encrypt the IoT data.

3.3.1. DNA encryption

The unique storage density of DNA as an information carrier makes it a better option for handling the challenge of producing or storing massive amounts of Pad. Utilizing DNA as an information carrier and contemporary biological processes as instruments, DNA cryptography fully utilizes the inherent benefits of high storage density and high parallelism to produce encryption. It is possible to replicate the encryption and decryption process as a biological or chemical reaction based on the double helix structure of DNA and the Watson-Crick complementary principle. After a substantial operation, it encodes the data and stores the plaintext, ciphertext, or other information on DNA encoding nucleotide sequence. The password mechanism has been developed by this point. Because so many DNA-based encryption algorithms have been developed in recent years, DNA cryptography is still in its infancy and lacks a comprehensive model and an effective verification method.

3.3.2 Key Select and the Plaintext Block

Key Select

The key in this encryption might be split into two pieces. (1). The selected gene sequence information, which is one component of the key, will be communicated over a secure channel between the sender and the recipient and will not be accessible to outside parties. The researcher establishes the beginning and ending points of the search position to improve algorithm security. The advantage of this approach is that it eliminates the requirement for entire gene sequence expression, and it saves money by limiting encryption and decryption operations to the crucial location of the key sequence from the point at which both parties agreed to begin. (2). As an additional component of the key, the Key Generator's beginning key is used to operate the device and produce a chaotic sequence. The two parameters μ and x in this section represent the key, as the Key Generator we built is based on Logistic Mapping.

Plaintext Block

The binary plaintext needs to be grouped into 32-bit chunks before encryption. When "GENEGRYPTOGRAPHY" is the plaintext, for instance, Group 1 will be "GENE", Group 2 will be "GRYP", Group 3 will be "TOGR", and Group 4 will be "APHY" until the plaintext is blocked. The plaintext ought to be filled in when its length is not divisible by four. The specific operation is as follows: We fill in the remaining space at the end of the plaintext after Mod 4. For example, we will insert three letters "3" at the end of the plaintext when the length of the plaintext mod 4 equals 3.

3.3.3 Encryption

Step 1 : The investigator determines at random the Initial Key key0, which consists of two double values, and sets them as the Logistic Mapping parameters (μ and x); In addition, the first encryption will use a 32-bit key1 generated by the Key Generator to encrypt plaintext. Then, following

converting plaintext into ASCII codes, the researchers should separate the participants into various groups; Lastly, the researcher ought to do an XOR operation between key1 and the 32-bit plaintext. The sequence m1 will be obtained by the researcher following these steps.

Step 2 : Initially m1 needs to be translated into DNA code in accordance with the DNA encoding described in 3.1. The researcher will obtain the 16-mer olio nucleotide DNA sequence se1 through encoding; Second, the unique DNA sequence (DNAseq) included in them will be obtained using the key and the provided DNA sequence information; Next, the researcher draws a random point x (0<x), from which the special string that matches m1 is found by searching the sequence. Four continuous bases mean that se11, se12, se13, and se14 can all be exactly the same as m1. The following will be returned: q1, q2, q3, q4; The points are then restored into the cipher-text array Pointer by the method.

Step 3 : A new encryption key key_m is generated by the Key Generator and is utilized in the subsequent encryption procedure. Moreover, the researcher ought to do an XOR operation on the 32-bit plaintext and key_m. Then, the new sequence n_m will appear.

Step 4 : Steps two and three should be carried out continuously until all plaintext has been encrypted. At that point, the program can be terminated. The process of decryption is the opposite of that of encryption.

3.3.4. DNA Symmetric Encryption Cryptosystem

Data including keys and DNA sequences should be sent over the secure channel by both the sender and the recipient. Sender uses a public channel to transmit ciphertext to the recipient. The receiver will utilize the DNA sequence information to determine the correct DNA sequence after receiving the cipher-text from the sender. The proper plaintext will then be retrieved by the recipient using the key and the decryption method.

3.3.5. Key Generator

1. Developing Chaos Sequence y: The key is provided by the values of the logistic parameters τ and x. The chaos sequence will be produced using formula 2:

$$y = (y1, y2, y3, \dots, yk) \quad (2)$$

2. Creating Key: The key yj will be chosen in the sequence y for each round. Formula (3) states that it will be changed into a 32-bit binary number:

$$[zj]2 = yj9 * 255 \quad (3)$$

3.Consequently, in each round, the key Z will be represented by formula (4):

$$z = [zj, zj + 1, zj + 2, zj + 3] \quad (4)$$

Reason: the chaotic sequence y is where the chaos value yj originated. 255 must be multiplied before it maps to 8-bit binary zj. Each consecutive four zj will be utilized as a single 32-bit key.

3.4. Cloud Layer

The cloud layer refers to the virtualized infrastructure that enables the delivery of computing services over the Internet. The part of the cloud computing infrastructure devoted to safely storing and managing data is referred to as the cloud data storage layer. It includes databases and distributed storage systems spread across several servers and data centres, offering scalable, dependable, and reasonably priced storage solutions. In this, the DNA-encrypted IoT datas are stored in the cloud layer.

4. RESULT AND DISCUSSION

The proposed method's experimental results are analyzed and discussion of performance is done in terms of numerous evaluation metrics in this section. The effectiveness of the proposed system has been assessed by using the MATLAB simulator with a 4 GB RAM and an i5 processor.

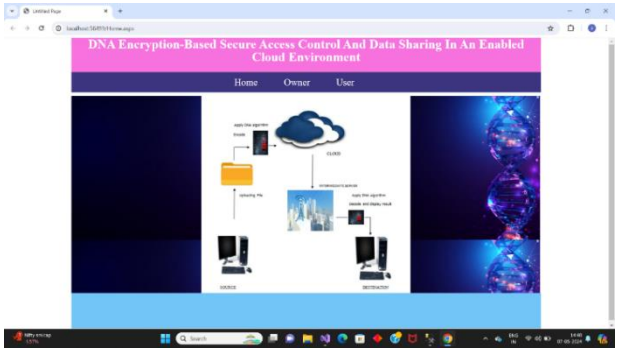

Figure 2. Home Page

Figure 2 shows the homepage. It is the home page of the DNA Encryption based Secure access control and Data sharing in an enabled cloud environment.

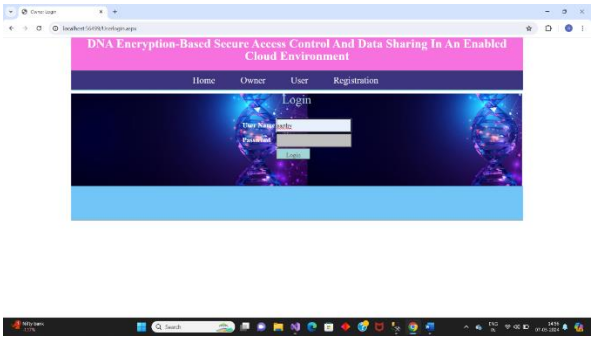

Figure 3. User Registration

Figure 3. shows the user registration page of the DNA Encryption based Secure access control and Data sharing in an enabled cloud environment in which the user gives the details for registration.

Figure 4 describes the Decrypted web page of the DNA Encryption based Secure access control and Data sharing in an enabled cloud environment

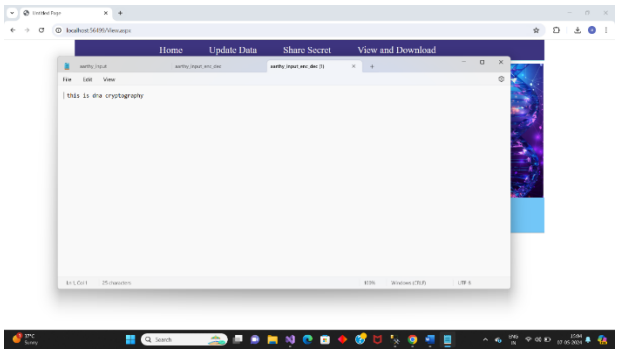

Figure 4. Decrypted web page

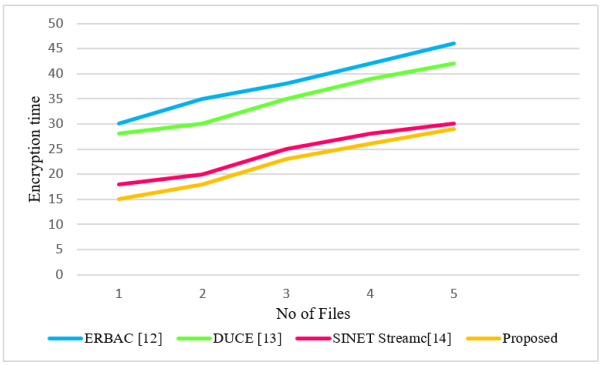

Figure 5. Comparison Analysis of Encryption Time

The encryption time of the proposed DESACS technique is compare with the existing methods. In this, the proposed DESACS technique takes less time to encrypt a file than the existing methods such as ERBAC [12], DUCE [13] and SINET Stream [14]. The proposed technique's encryption time is 72.07%, 56.92%, and 9.04% faster than that of the existing methodologies (Figure 5).

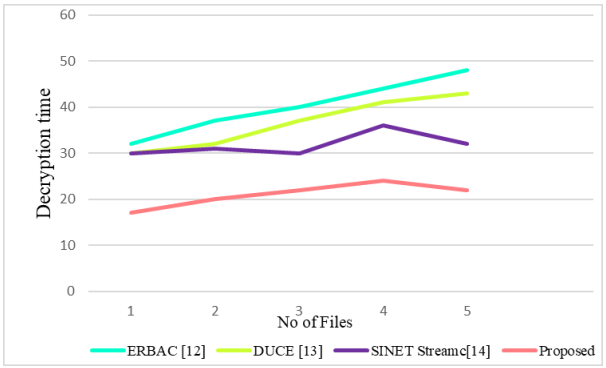

Figure 6. Comparison Analysis of Decryption Time

Figure 6. describes the decryption time comparison of the proposed DESACS with the existing method. The proposed method takes less time consumption than the existing methods. The decryption time of the proposed technique is 82.7%, 63.36%, and 19.09% faster than that of the existing techniques.

In Figure. 7, the proposed system and the existing techniques such as ERBAC [12], DUCE [13], and SINET Stream [14] are contrasted for the execution time. In this, the proposed DESACS takes less time for execution than the existing methods.

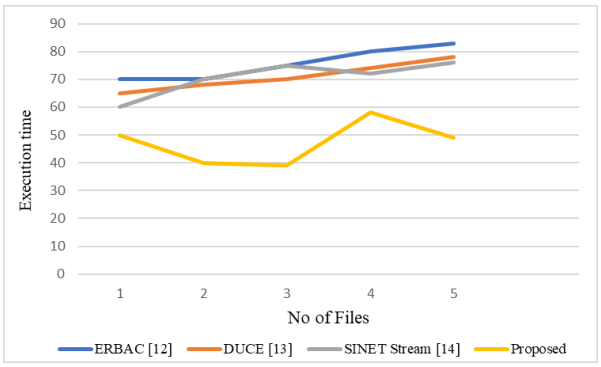

Figure 7. Comparison Analysis Execution time

5. CONCLUSION

A DNA Encryption-based Secure Access Control and Sharing (DESACS) technique in an IoT-enabled Cloud environment which enhances the privacy and security of IoT data. Initially, the IoT layer represents the devices in the Internet of Things (IoT) ecosystem. These devices (labelled D1 to DN) are connected to gateways. The gateways act as intermediaries, facilitating communication between the devices and other layers. Then the Authentication is a crucial step to ensure that only authorized devices and data can proceed further. The pink hexagon labelled "Authenticated Filtering" likely represents a mechanism for verifying the identity of devices or data streams. Devices that pass authentication can move on to the next layer. The Data encryption improves data security. Data might have been encrypted using DNA sequences in a process known as "DNA-based encryption," which would be challenging to decode without the right key. Finally, the top layer Cloud data storage provides scalability, accessibility, and redundancy. The proposed secure data transmission scheme will be extended to work in an uncontrolled environment in future by replacing increasing security challenges in cloud computing while ensuring data confidentiality and privacy in a globally connected digital ecosystem.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] P. Goyal, A.K. Sahoo, and T.K. Sharma, "Internet of things: Architecture and enabling technologies", Materials Today: Proceedings, vol. 34, pp.719-735, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] L. Kong, and B. Ma, "Intelligent manufacturing model of construction industry based on Internet of Things technology", *The International Journal of Advanced Manufacturing Technology*, vol. 107, no. 3, pp.1025-1037, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] E. Bazgir, E. Haque, N.B. Sharif, and M.F. Ahmed, "Security aspects in IoT based cloud computing", *World Journal of Advanced Research and Reviews*, vol. 20, no. 3, pp.540-551, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] S. Nguyen, Z. Salcic, X. Zhang, and A. Bisht, "A low-cost two-tier fog computing testbed for streaming IoT-based applications", *IEEE Internet of Things Journal*, vol. 8, no. 8, pp.6928-6939, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] N. Muthukumaran, N. Ruban Guru Prasath, R. Kabilan, "Driver Sleepiness Detection Using Deep Learning Convolution Neural Network Classifier", *Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Palladam, India*, pp. 386-390, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] A.T. Atieh, "The next generation cloud technologies: a review on distributed cloud, fog and edge computing and their opportunities and challenges", *ResearchBerg Review of Science and Technology*, vol. 1, no. 1, pp.1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] R. Joshua Samuel Raj, T. Sudarson Rama Perumal, N. Muthukumaran, D.R. Ganesh, "Rapid Efficient Loss Less Color Image Compression Using RCT Technique and Hierarchical Prediction", In: Peter, J.D., Fernandes, S.L., Alavi, A.H. (eds) "Disruptive Technologies for Big Data and Cloud Applications", *Lecture Notes in Electrical Engineering*, vol. 905, pp. 189–202, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] F. Jauro, H. Chiroma, A.Y. Gital, M. Almutairi, M.A. Shafi'i, and J.H. Abawajy, "Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend", *Applied Soft Computing*, vol. 96, pp.106582, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies", *IEEE Access*, vol. 9, pp. 57792-57807, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] A. Karthika, N. Muthukumaran, and R. Joshua Samuel Raj, "An Ads-Csab Approach for Economic Denial of Sustainability Attacks in Cloud Storage", *International Journal of Scientific & Technology Research*, vol. 9, no. 04, pp. 2575-2578, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] G. Deep, J. Sidhu, and R. Mohana, "Insider threat prevention in distributed database as a service cloud environment", *Computers & Industrial Engineering*, vol. 169, pp.108278, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] M. Rashid, S.A. Parah, A.R. Wani, and S.K. Gupta, "Securing E-Health IoT data on cloud systems using novel extended role-based access control model", *Internet of Things (IoT) Concepts and Applications*, pp.473-489, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] N. Shi, B. Tang, R. Sa ndhu, and Q. Li, "DUCE: distributed usage control enforcement for private data sharing in the Internet of Things", *In Data and Applications Security and Privacy XXXV*: 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, Canada, July 19–20, 2021, Proceedings 35, pp. 278-290, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] N. Kitagawa, A. Takefusa, and K. Aida, "Development of a Secure Data Sharing Mechanism for IoT Application Systems", *In 2022 IEEE 11th International Conference on Cloud Networking (CloudNet)*, pp. 131-135, 2022. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Fugkeaw, L. Wirz, and L. Hak, "Secure and Lightweight Blockchain-enabled Access Control for Fog-Assisted IoT Cloud-based Electronic Medical Records Sharing", *IEEE Access*. 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] S. Liu, L. Chen, H. Yu, S. Gao, and H. Fang, "BP-AKAA: blockchain-enforced privacy-preserving authentication and key agreement and access control for IoT", *Journal of Information Security and Applications*, vol. 73, p.103443, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] P. Han, Z. Zhang, S. Ji, X. Wang, L. Liu, and Y. Ren, "Access control mechanism for the Internet of Things based on blockchain and inner product encryption", *Journal of Information Security and Applications*, vol. 74, pp.103446, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] A. Singh, A. Kumar, and S. Namasudra, "DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography", *Frontiers of Computer Science*, vol. 18, no. 1, pp.181801, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

A.R. Aarthy she was born in Kanyakumari district, Tamil Nadu, India in 1999.She received her BE degree in Computer Science and Engineering from Satyam college of Engineering and Technology, Aralvaimozhi, Anna University, currently she is pursuing her ME degree in Computer Science and Engineering from Satyam College of Engineering and Technology, Aralvaimozhi, Anna University, India. Her interested research area is cloud computing, and Internet of Things.

K. Vinoth Kanth received his B.tech in Information Technology from Sun college of engineering and technology, Anna University, in 2009 and obtained M.E degree in CSE from University college of engineering Nagercoil in 2013. His interested research area is Image processing and cloud computing.

Arrived: 17.05.2024
Accepted: 08.06.2024