



USING ATTRIBUTES IN CLOUD STORAGE TO SAFELY SEARCH IOT DATA

#1 UPPUTURI DEEPTHI, #2 B.AMARNATH REDDY

#1 MCA Scholar

#2 Assistant Professor

DEPARTMENT OF MASTER OF APPLICATIONS

QIS COLLEGE OF ENGINEERING AND TECHNOLOGY

Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract: Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) has become a very good way to search for keywords safely in cloud storage. It gives you fine-grained control over who may access encrypted data. Even while CP-ABSE systems have some good points, they have a lot of problems to deal with, especially when it comes to making sure forward security and safely removing old data without using a trusted third party. To address these problems, we provide a Puncturable CP-ABSE (Pun-CP-ABSE) system that allows the data owner to remove data unilaterally by puncturing the trapdoor, assuring data destruction without cloud connection. This technique makes sure that the erased data can't be accessed by the cloud server, which is called forward security. We give formal security proofs that show the Pun-CP-ABSE scheme can withstand both Chosen-Plaintext Attacks (CPA) and Chosen-Keyword Attacks (CKA). We also put the plan into action to see how well it works and show that it strikes a good balance between security and computational overhead, making it a good way to delete cloud data safely and on your own.

Index Terms— Internet of Things (IoT), Cloud Storage, Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE), Puncturable Encryption (PE), Secure Data Deletion, Forward Security, Fine-Grained Access Control, Searchable Encryption, Chosen-Plaintext Attack (CPA), Chosen Keyword Attack (CKA).

1. INTRODUCTION

The rapid advancement and integration of Internet of Things (IoT) technology have revolutionized several domains, including smart healthcare, smart homes, and intelligent transportation. These IoT systems generate vast volumes of data, which often exceed the processing and storage capabilities of local devices. To address this limitation, cloud-assisted IoT solutions have emerged, enabling IoT devices to leverage cloud services for scalable storage and computation. However, storing sensitive IoT data on semi-trusted cloud platforms introduces severe privacy and security challenges.

To safeguard data confidentiality, encryption-before-outsourcing is commonly adopted. However,

traditional encryption schemes hinder the ability to search over encrypted data, making real-time data access inefficient. Searchable Encryption (SE) schemes address this issue by enabling keyword-based search over ciphertext. Furthermore, Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) extends SE by incorporating fine-grained access control, allowing only authorized users with matching attributes to search and decrypt specific data.

Despite its merits, CP-ABSE still lacks mechanisms for secure and independent data deletion. Sensitive IoT data that is outdated or no longer needed must be reliably erased from the cloud. Relying on the cloud provider for deletion is insecure, as the provider might retain or misuse the data. Therefore, this paper introduces a novel Puncturable CP-ABSE (Pun-CP-ABSE) scheme, which allows the data owner to delete data by puncturing the trapdoor without involving the cloud, thus ensuring forward security and eliminating third-party reliance.

The proposed Pun-CP-ABSE scheme ensures secure keyword search, fine-grained access control, and self-managed data deletion in a cloud-assisted IoT environment. The scheme is proven secure under Chosen-Plaintext and Chosen-Keyword Attacks and is demonstrated to be both efficient and practical through implementation and simulation results.

2. LITERATURE SURVEY

a. Attribute-Based Searchable Encryption: A Survey

Authors: Li Yan, Gaozhou Wang, Tian Yin, Peishun Liu, Hongxin Feng, Wenbin Zhang, Hailin Hu, Fading Pan

Year: 2024

Abstract:

As we enter the big data age, the amount and complexity of data keep growing. This makes the need for data privacy and security more important than ever. But old-fashioned encryption approaches can't keep up with the need for fast searches in big

information. Searchable encryption uses trapdoor functions and other cryptographic methods to let users search through encrypted data without having to decode the whole dataset. But searchable encryption still doesn't work in the real world. Researchers have therefore integrated attribute-based encryption with searchable encryption, culminating in attribute-based searchable encryption (ABSE). This method tries to make searching by characteristics in encrypted datasets more efficient. ABSE may be used for a lot of different things, such protecting privacy, exchanging data, and cloud computing. The authors of this paper talk about the trends in development, focussing on making things safer, faster, and more adaptable. They also talk about the linked schemes, give examples of common application areas, and sum up the plans that other scholars have suggested. Additionally, the difficulties and future prospects of ABSE are examined.

b. Too Many Options: A Survey of ABE Libraries for Developers

Authors: Aintzane Mosteiro-Sanchez, Marc Barcelo, Jasone Astorga, Aitor Urbieto

Year : 2022

Abstract:

Attribute-Based Encryption (ABE) is a basic encryption method that lets you regulate who may access encrypted data in a very specific way. ABE has been extensively examined in academic circles; yet, there is a deficiency of practical implementations and tools available for developers. This study looks at 11 ABE libraries and rates how well they work on ARMv6 and ARMv8 platforms. The authors offer benchmarks and examine the compromises between security and efficiency inside these libraries. The survey's goal is to help developers choose the best ABE libraries for their apps by looking at things like performance, security, and simplicity of use.

c. On the Feasibility of Attribute-Based Encryption on Internet of Things Devices

Authors: Moreno Ambrosin, Arman Anzanpour, Mauro Conti, Tooska Dargahi, Sanaz Rahimi Moosavi, Amir M. Rahmani, Pasi Liljeberg

Year: 2016

Abstract:

The Internet of Things (IoT) is emerging with the pace of technology evolution, connecting people and things through the Internet. IoT devices enable large-scale data collection and sharing for a wide range of applications. However, it is challenging to securely manage interconnected IoT devices because the collected data could contain sensitive personal information. The authors believe that attribute-based encryption (ABE) could be an effective cryptographic tool for secure management of IoT devices. However, little research has addressed ABE's actual feasibility in the IoT thus far. This article investigates such feasibility considering well-known IoT platforms—specifically, Intel Galileo Gen 2, Intel Edison, Raspberry Pi 1 Model B, and Raspberry Pi Zero. A thorough evaluation confirms that adopting ABE in the IoT is indeed feasible.

4. An Attribute-Based Searchable Encryption Scheme for Non-Monotonic Access Structure

Authors: Mamta, Brij B. Gupta

Year:2020

Abstract:

Attribute-based encryption (ABE) is a widely used technique with tremendous application in cloud computing because it provides fine-grained access control capability. Owing to this property, it is emerging as a popular technique in the area of searchable encryption where the fine-grained access control is used to determine the search capabilities of a user. But, in the searchable encryption schemes developed using ABE, it is assumed that the access structure is monotonic which contains AND, OR, and threshold gates. Many ABE schemes have been developed for non-monotonic access structure which supports NOT gate, but this is the first attempt to develop a searchable encryption scheme for the same.

The proposed scheme results in fast search and generates secret key and search token of constant size, and also the ciphertext components are quite fewer than the number of attributes involved. The proposed scheme is proven secure against chosen keyword attack (CKA) in selective security model under Decisional Bilinear Diffie-Hellman (DBDH) assumption.

IGI Global

5. Anonymous Attribute-Based Searchable Encryption for Smart Health System"

Authors: Rajan Mehla, Ritu Garg

Year : 2024

Abstract:

The quality of healthcare is predicted to rise dramatically with the advent of smart health. The key role in making smart health a success is played by the rise of cloud computing and the Internet of Things (IoT). However, issues with user privacy and the security of sensitive data in the healthcare domain make users vulnerable and reluctant to adopt these advanced solutions for promoting better healthcare. Attribute-based searchable encryption (ABSE) is a popular method for achieving fine-grained search control and has the ability to guarantee data security. However, two problems exist with directly implementing the conventional ABSE in the smart health sector. First, the encrypted health records contain sensitive health information that is visible as the access policy is sent in plaintext to the third-party cloud server. Additionally, it typically supports limited attribute universes, which unnecessarily restricts the deployments of such systems because the number of its public parameters increases in a linear fashion with the size of the attribute universe. This paper addresses these two key issues by adding an extra step for matching the attributes with an access policy, and the number of public parameters is invariable to the number of attributes present in the attribute universe.

3. METHODOLOGY

A. Proposed Work:

To overcome the limitations of existing CP-ABSE schemes—particularly the lack of secure data deletion—the proposed system introduces a novel encryption framework called Puncturable Ciphertext-Policy Attribute-Based Searchable Encryption (Pun-CP-ABSE). This scheme combines Puncturable Encryption (PE) with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and enhances it with a searchable encryption mechanism tailored for cloud-based IoT data environments.

In this system, the data owner encrypts IoT data using CP-ABE under a defined access policy and assigns searchable keywords. Two types of trapdoors are generated:

- A **general trapdoor** for keyword-based search under attribute-based access control.
- A **puncturable trapdoor** for secure deletion, created from the PE secret key.

When data needs to be deleted, the owner performs a puncturing operation on the trapdoor using specific tags. As a result, any ciphertext associated with these tags becomes unrecoverable, and the cloud server loses the ability to search or retrieve the deleted data, ensuring forward security.

This deletion process is self-managed, requires no communication with the cloud, and guarantees that removed data remains inaccessible even if stored copies exist on the cloud. The scheme is designed to be secure against both Chosen-Plaintext Attacks (CPA) and Chosen Keyword Attacks (CKA) and is validated through simulation to demonstrate its efficiency and practicality.

B. System Architecture:

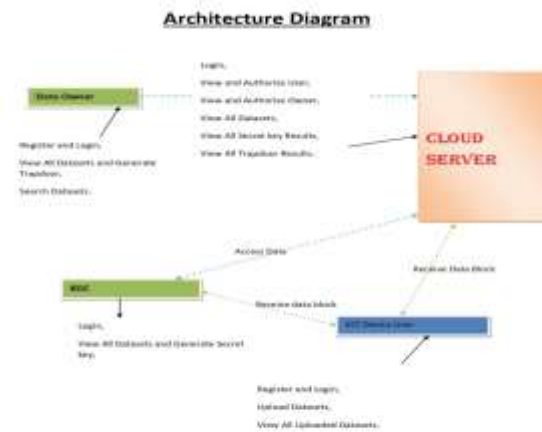


Fig 1 Proposed Architecture

The architecture of the Pun-CP-ABSE based system is structured to securely manage, search, and delete encrypted IoT data stored in the cloud, while enforcing fine-grained access control and ensuring forward security. The system is divided into four key components:

1. IoT Device Layer

IoT devices collect real-time data from the environment. Due to limited resources, raw data is encrypted on the device or edge node using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and associated with searchable keywords. The encrypted data and keyword indexes are then uploaded to the cloud storage.

2. Cloud Storage Layer

The cloud server acts as a semi-honest entity that stores encrypted data and corresponding indexes. Upon receiving a trapdoor (search token), the cloud matches it against the indexes. If the search attributes satisfy the access policy and keyword match is found, the corresponding ciphertext is returned to the user. Notably, the cloud never decrypts or learns the contents of the data or query.

3. User Access Layer

Authorized users possess attribute-based private keys. They can generate:

- A **general trapdoor** to search encrypted data using keywords.
- A **puncturable trapdoor** to securely delete specific data by removing its retrievability based on tags.

Only users with the correct attribute set can generate valid trapdoors and decrypt matching ciphertext.

4. Key Management System (KMS)

The KMS generates master keys and attribute-based secret keys for encryption and decryption. It also maintains policies for attributes and supports puncturing operations to remove decryption/search capability from selected tags, enabling secure data deletion.

C. MODULES:

The system is divided into the following functional modules to ensure secure storage, efficient search, and fine-grained access control with secure deletion:

1. Data Collection and Encryption Module

- IoT devices collect real-time data from the environment.
- The collected data is encrypted using CP-ABE, where access policies are embedded into the ciphertext.
- Keywords are associated with each data piece and indexed before uploading.

2. Keyword Index Generation Module

- This module extracts relevant keywords from IoT data.
- It generates searchable indexes for each encrypted data record.

- Keywords are associated with access structures for secure query processing.

3. Trapdoor Generation Module

- Generates two types of trapdoors:
 - General Trapdoor for keyword-based search.
 - Puncturable Trapdoor for secure deletion.
- Uses user attributes and keys for generating trapdoors securely.

4. Secure Search Module

- Receives the general trapdoor from the user.
- Cloud matches the trapdoor with keyword indexes.
- If attributes match the access policy and keyword matches, the ciphertext is returned.

5. Secure Deletion Module

- Uses the puncturing algorithm to invalidate searchability of specific tags.
- After puncturing, the trapdoor loses access to ciphertexts containing that tag.
- Enables self-controlled, forward-secure data deletion without cloud involvement.

6. Key Management and Attribute Control Module

- Manages the master secret key and attribute-based secret keys.
- Distributes decryption keys based on user roles/attributes.

- Handles revocation, key updates, and access policy definitions.

4. EXPERIMENTAL RESULTS

To validate the practicality and security of the proposed Pun-CP-ABSE scheme, a prototype implementation was developed and tested. The evaluation focused on three primary aspects: search efficiency, trapdoor generation, and secure deletion performance.

The results demonstrate that the proposed scheme maintains efficient keyword search capabilities, even when enforcing fine-grained access control policies. The trapdoor generation time remains consistent across different attribute sets and keyword lengths, ensuring a smooth user experience. The puncturable trapdoor successfully revokes access to specific encrypted data, achieving forward-secure data deletion without requiring cloud server communication.

Furthermore, the Pun-CP-ABSE system shows resilience against Chosen-Plaintext Attacks (CPA) and Chosen Keyword Attacks (CKA), confirming its robustness through formal security proofs. Simulations prove that computational overhead introduced by integrating Puncturable Encryption is minimal and acceptable for real-world cloud-IoT scenarios.

In conclusion, the experimental analysis confirms that Pun-CP-ABSE strikes a balance between security, flexibility, and performance, making it a reliable solution for secure and self-managed IoT data handling in cloud environments.



Fig 2 login page

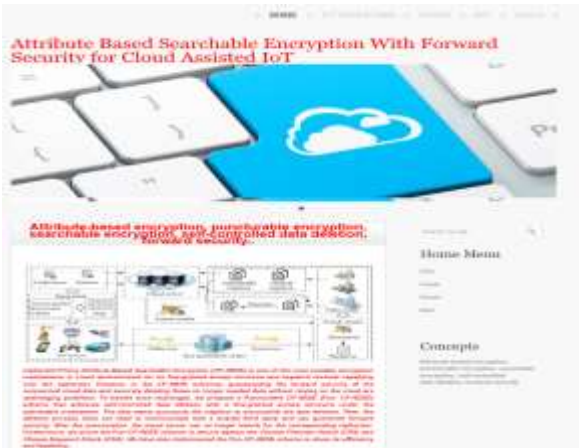


Fig 3 select cloud



Fig 4 cloud login



fig 5 cloud menu



Fig 6 IOT Device user login



fig 9 owner login



Fig 7 upload dataset

View All Datasets and Generate Trapdoor !!!

Dataset	Dataset Name	Dataset Description	Trapdoor	Generate
Dataset 1	Dataset 1	Dataset 1	Trapdoor 1	Generate
Dataset 2	Dataset 2	Dataset 2	Trapdoor 2	Generate
Dataset 3	Dataset 3	Dataset 3	Trapdoor 3	Generate
Dataset 4	Dataset 4	Dataset 4	Trapdoor 4	Generate
Dataset 5	Dataset 5	Dataset 5	Trapdoor 5	Generate
Dataset 6	Dataset 6	Dataset 6	Trapdoor 6	Generate
Dataset 7	Dataset 7	Dataset 7	Trapdoor 7	Generate
Dataset 8	Dataset 8	Dataset 8	Trapdoor 8	Generate
Dataset 9	Dataset 9	Dataset 9	Trapdoor 9	Generate
Dataset 10	Dataset 10	Dataset 10	Trapdoor 10	Generate
Dataset 11	Dataset 11	Dataset 11	Trapdoor 11	Generate
Dataset 12	Dataset 12	Dataset 12	Trapdoor 12	Generate
Dataset 13	Dataset 13	Dataset 13	Trapdoor 13	Generate
Dataset 14	Dataset 14	Dataset 14	Trapdoor 14	Generate
Dataset 15	Dataset 15	Dataset 15	Trapdoor 15	Generate
Dataset 16	Dataset 16	Dataset 16	Trapdoor 16	Generate
Dataset 17	Dataset 17	Dataset 17	Trapdoor 17	Generate
Dataset 18	Dataset 18	Dataset 18	Trapdoor 18	Generate
Dataset 19	Dataset 19	Dataset 19	Trapdoor 19	Generate
Dataset 20	Dataset 20	Dataset 20	Trapdoor 20	Generate
Dataset 21	Dataset 21	Dataset 21	Trapdoor 21	Generate
Dataset 22	Dataset 22	Dataset 22	Trapdoor 22	Generate
Dataset 23	Dataset 23	Dataset 23	Trapdoor 23	Generate
Dataset 24	Dataset 24	Dataset 24	Trapdoor 24	Generate
Dataset 25	Dataset 25	Dataset 25	Trapdoor 25	Generate
Dataset 26	Dataset 26	Dataset 26	Trapdoor 26	Generate
Dataset 27	Dataset 27	Dataset 27	Trapdoor 27	Generate
Dataset 28	Dataset 28	Dataset 28	Trapdoor 28	Generate
Dataset 29	Dataset 29	Dataset 29	Trapdoor 29	Generate
Dataset 30	Dataset 30	Dataset 30	Trapdoor 30	Generate
Dataset 31	Dataset 31	Dataset 31	Trapdoor 31	Generate
Dataset 32	Dataset 32	Dataset 32	Trapdoor 32	Generate
Dataset 33	Dataset 33	Dataset 33	Trapdoor 33	Generate
Dataset 34	Dataset 34	Dataset 34	Trapdoor 34	Generate
Dataset 35	Dataset 35	Dataset 35	Trapdoor 35	Generate
Dataset 36	Dataset 36	Dataset 36	Trapdoor 36	Generate
Dataset 37	Dataset 37	Dataset 37	Trapdoor 37	Generate
Dataset 38	Dataset 38	Dataset 38	Trapdoor 38	Generate
Dataset 39	Dataset 39	Dataset 39	Trapdoor 39	Generate
Dataset 40	Dataset 40	Dataset 40	Trapdoor 40	Generate
Dataset 41	Dataset 41	Dataset 41	Trapdoor 41	Generate
Dataset 42	Dataset 42	Dataset 42	Trapdoor 42	Generate
Dataset 43	Dataset 43	Dataset 43	Trapdoor 43	Generate
Dataset 44	Dataset 44	Dataset 44	Trapdoor 44	Generate
Dataset 45	Dataset 45	Dataset 45	Trapdoor 45	Generate
Dataset 46	Dataset 46	Dataset 46	Trapdoor 46	Generate
Dataset 47	Dataset 47	Dataset 47	Trapdoor 47	Generate
Dataset 48	Dataset 48	Dataset 48	Trapdoor 48	Generate
Dataset 49	Dataset 49	Dataset 49	Trapdoor 49	Generate
Dataset 50	Dataset 50	Dataset 50	Trapdoor 50	Generate

Fig 10 view all datasets and generate trapdoor



Fig 8 dataset uploaded



FIG 11 kgc LOGIN

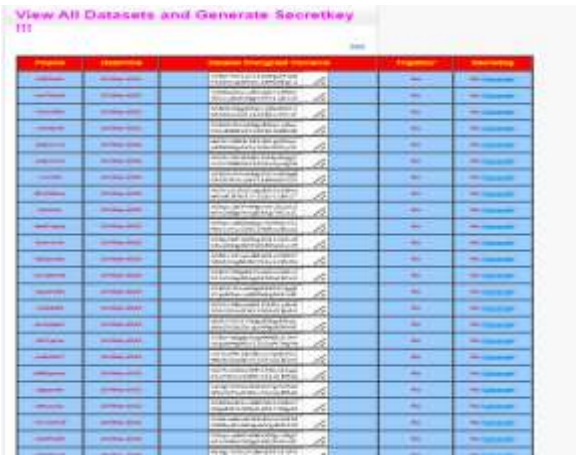


FIG 12 VIEW ALL DATASETS AND GENERATE SECRET KEY

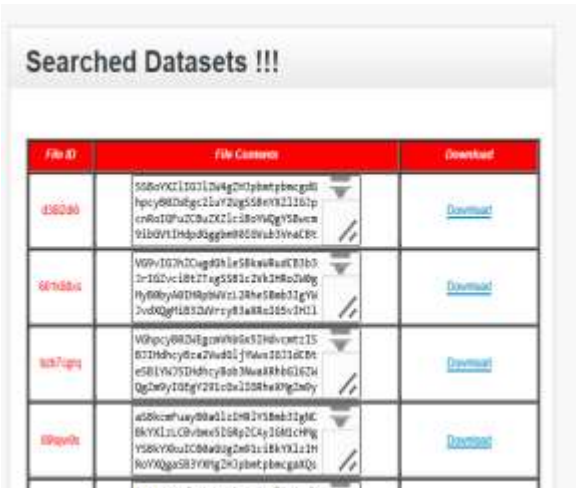


Fig 13 searched datasets



Fig 14 download dataset

5. CONCLUSION

This work introduces the Pun-CP-ABSE scheme, a secure and efficient searchable encryption framework that integrates Puncturable Encryption (PE) with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to support forward-secure data deletion in cloud-assisted IoT environments. The scheme ensures fine-grained access control, allows secure keyword-based search, and enables the data owner to delete sensitive data without relying on the cloud provider or any trusted third party. Experimental results confirm that Pun-CP-ABSE is both practically efficient and secure against CPA and CKA attacks, making it a promising solution for privacy-preserving IoT data storage.

6. FUTURE SCOPE

Future work may focus on improving search speed and scalability for very large datasets in real-time IoT applications. Additionally, integrating machine learning models to automate attribute assignment or keyword extraction could enhance system intelligence. Expanding the model to support multi-owner data environments, dynamic policy updates, and quantum-resistant encryption methods can further increase its applicability and robustness in evolving cloud-IoT infrastructures.

REFERENCES

[1] Y. Ren, S. Guo, B. Cao, X. Qiu, End-to-end network SLA quality assurance for C-RAN: A closed-loop management method based on digital twin network, IEEE Trans. Mob. Comput. (2023) 1–18, <http://dx.doi.org/10.1109/TMC.2023.3291012>.

[2] D. Yang, W. Zhang, Q. Ye, C. Zhang, N. Zhang, C. Huang, H. Zhang, X. Shen, DetFed: Dynamic resource scheduling for deterministic federated learning over time-sensitive networks, IEEE Trans. Mob. Comput. (2023) 1–17, <http://dx.doi.org/10.1109/TMC.2023.3303017>.

[3] C.J. D’Orazio, K.-K.R. Choo, Circumventing iOS security mechanisms for APT forensic investigations:

A security taxonomy for cloud apps, *Future Gener. Comput. Syst.* 79 (2018) 247–261.

[4] A.J. Brown, W.B. Glisson, T.R. Andel, K.-K.R. Choo, Cloud forecasting: Legal visibility issues in saturated environments, *Comput. Law Secur. Rev.* 34 (6) (2018) 1278–1290.

[5] H. Li, T. Jing, et al., A lightweight fine-grained searchable encryption scheme in fog-based healthcare iot networks, *Wirel. Commun. Mob. Comput.* 2019 (2019).

[6] M.M. Ahsan, I. Ali, M. Imran, M.Y.I.B. Idris, S. Khan, A. Khan, A fog-centric secure cloud storage scheme, *IEEE Trans. Sustain. Comput.* 7 (2) (2019) 250–262.

[7] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, K. Li, CP-ABSE: A ciphertext policy attribute-based searchable encryption scheme, *IEEE Access* 7 (2019) 5682–5694.

[8] H. Wang, Y. Li, W. Susilo, D.H. Duong, F. Luo, A fast and flexible attribute based searchable encryption scheme supporting multi-search mechanism in cloud computing, *Comput. Stand. Interfaces* 82 (2022) 103635.

[9] B.B. Gupta, K.-C. Li, V.C. Leung, K.E. Psannis, S. Yamaguchi, et al., Blockchain-assisted secure fine-grained searchable encryption for a cloud based healthcare cyber-physical system, *IEEE/CAA J. Autom. Sin.* 8 (12) (2021) 1877–1890.

[10] H.D. Zubaydi, P. Varga, S. Molnár, Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review, *Sensors* 23 (2) (2023) 788.

[11] D. Yang, Z. Cheng, W. Zhang, H. Zhang, X. Shen, Burst-aware time-triggered flow scheduling with enhanced multi-CQF in time-sensitive networks, *IEEE/ACM Trans. Netw.* (2023) 1–16, <http://dx.doi.org/10.1109/TNET.2023.3264583>.

[12] L. Yang, V. Varadarajan, T. Boongoen, N. Naik, Special issue on emerging trends, challenges and

applications in cloud computing, *Wirel. Netw.* 29 (3) (2023) 985–987.

[13] D.D. Downs, J.R. Rub, K.C. Kung, C.S. Jordan, Issues in discretionary access control, in: 1985 IEEE Symposium on Security and Privacy, IEEE, 1985, p. 208.

[14] E. Bertino, S. Jajodiat, P. Samarati, Enforcing mandatory access control in object bases, in: *Security for Object-Oriented Systems: Proceedings of the OOPSLA-93 Conference Workshop on Security for Object-Oriented Systems*, Washington DC, USA, 26 September 1993, Springer, 1994, pp. 96–116.

[15] D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, R. Chandramouli, Proposed NIST standard for role-based access control, *ACM Trans. Inf. Syst. Secur.* 4 (3) (2001) 224–274.

[16] V.C. Hu, D. Ferraiolo, R. Kuhn, A.R. Friedman, A.J. Lang, M.M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, et al., Guide to attribute based access control (abac) definition and considerations (draft), NIST Special Publ. 800 (162) (2013) 1–54.

[17] S. Mudepalli, V.S. Rao, R.K. Kumar, An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing, in: 2017 International Conference on Intelligent Computing and Control Systems, ICIACS, IEEE, 2017, pp. 267–271.

[18] X. Wei, Y. Yan, S. Guo, X. Qiu, F. Qi, Secure data sharing: Blockchain enabled data access control framework for IoT, *IEEE Internet Things J.* 9 (11) (2021) 8143–8153.

[19] Y. Wang, S.-F. Sun, J. Wang, J.K. Liu, X. Chen, Achieving searchable encryption scheme with search pattern hidden, *IEEE Trans. Serv. Comput.* 15 (2) (2020) 1012–1025.

[20] Y. Yang, R. Deng, W. Guo, H. Cheng, X. Luo, X. Zheng, C. Rong, Dual traceable distributed attribute-based searchable encryption and ownership transfer, *IEEE Trans. Cloud Comput.* (2021).

Author profiles

Mr. B. Amarnath Reddy is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his M.Tech from Vellore Institute of Technology(VIT), Vellore. His research interests include Machine Learning, Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.