INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A., Google Scholar, Indian Citation Index (ICI), J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)], Index Copernicus Publishers Panel, Poland with IC Value of 5.09 (2012) & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **7835 Cities** in **197 countries/territories** are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to the recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript titled '_____' for likely publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published anywhere in any language fully or partly, nor it is under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to inclusion of their names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation/Post*	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

* i.e. Alumnus (Male Alumni), Alumna (Female Alumni), Student, Research Scholar (M. Phil), Research Scholar (Ph. D.), JRF, Research Assistant, Assistant Lecturer, Lecturer, Senior Lecturer, Junior Assistant Professor, Assistant Professor, Senior Assistant Professor, Co-ordinator, Reader, Associate Professor, Professor, Head, Vice-Principal, Dy. Director, Principal, Director, Dean, President, Vice Chancellor, Industry Designation **etc**. ***The qualification of author is not acceptable for the purpose***.

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of the mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) Only the **Abstract will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty-four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of the manuscript, within two days of its submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except on the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be typed in **bold letters**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT:** Abstract should be in **fully Italic printing**, ranging between **150** to **300 words**. The abstract must be informative and elucidating the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.

6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations etc.

7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php. However, mentioning of JEL Code is not mandatory.

8. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical, spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.

9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably be in ***2000 to 5000 WORDS***, But the limits can vary depending on the nature of the manuscript.

12. **FIGURES & TABLES**: These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self-explained, and the **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE**: These should be consecutively numbered in parenthesis, left aligned with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word may be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS**: These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section e.g. Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES**: The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they may follow Harvard Style of Referencing. **Also check to ensure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc., in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italic printing. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders before the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SECURE DATA MANAGEMENT MODEL (SDMM): ACCESS POLICY HIDING FOR EFFICIENT SHARING AND REVOCATION USING BLOCKCHAIN

BATTULA V. SATISH BABU
RESEARCH SCHOLAR, JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, HYDERABAD & ASST PROFESSOR
PRASAD V. POTLURI SIDDHARTHA INSTITUTE OF TECHNOLOGY
VIJAYAWADA

Dr. KARE SURESH BABU
PROFESSOR
SCHOOL OF IT
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY
HYDERABAD

ABSTRACT

In today's context, the secure sharing of sensitive data is paramount for maintaining privacy and confidentiality. Additionally, efficient revocation mechanisms play a vital role in promptly revoking access privileges to prevent unauthorized usage. Our work addresses these concerns by leveraging blockchain technology to share Attribute-Based Encrypted (ABE) ciphertext, which includes an IPFS file URL, access policies, and a revocation list. By incorporating a tree-based revocation mechanism and integrating Attribute-Based Access Control (ABAC) through smart contracts, such as OAMC, SAMC, ACC, and RMC, we ensure the seamless execution of necessary operations. Our system not only protects access policies but also enhances the efficiency of the revocation mechanism. Through extensive experimental evaluation and analysis, we have demonstrated the better performance of our methods compared to existing approaches.

KEYWORDS

ABE, ABAC, tree, revocation, IPFS, Blockchain.

JEL CODES

D82, D85, L86.

1. INTRODUCTION

To ensure the protection of sensitive information and maintain privacy, secure data sharing is crucial. It prevents unauthorized access and safeguards data from potential breaches. Additionally, efficient revocation mechanisms are necessary to promptly revoke access privileges, preventing unauthorized usage and maintaining control over shared data, thereby enhancing overall data security. These objectives can be achieved by leveraging attribute-based mechanisms such as Attribute-Based Encryption (ABE) and Attribute-Based Access Control (ABAC), in combination with blockchain technology, which adds an extra layer of transparency and immutability to the sharing and revocation processes.

Blockchain operates through the integration of cryptographic principles, decentralized architecture, and distributed consensus. Transactions are organized into blocks and connected using cryptographic hashes, forming an unchangeable data chain. Once a block is added, it becomes nearly impossible to alter, ensuring transparency, security, and trust in the system. Consensus algorithms like Proof of Work or Proof of Stake validate and establish agreement among participants on the blockchain's state. The immutability of added blocks ensures transparency, security, and a trustworthy system.

Attribute-Based Encryption (ABE) is a cryptographic method that facilitates access control by leveraging attributes. It enables the encryption of data with specific attributes, ensuring that only users possessing corresponding attributes can decrypt and access the information. ABE empowers fine-grained access control, offering flexibility and customization in the secure sharing of encrypted data.

Attribute-Based Access Control (ABAC) is a security framework that governs access to resources based on associated attributes of users, objects, and the environment. ABAC enables detailed control by considering multiple attributes concurrently, resulting in accurate and context-aware access decisions. This model offers a fine-grained level of access control, ensuring that resources are only accessible to authorized entities based on their attribute values.

In the realm of access control and data protection, ABE (Attribute-Based Encryption) and ABAC (Attribute-Based Access Control) are interconnected yet separate concepts. ABE primarily deals with encryption and decryption, ensuring secure data storage and sharing. In contrast, ABAC functions as an access control model, making access decisions based on various attributes associated with resources.

In this paper, we have used both ABE, ABAC mechanisms on blockchain along with offline storage IPFS and proposed a model to realize efficient sharing and revoking mechanisms. This paper makes three distinct contributions, which are outlined as follows:

- Outsourced storage for data owner in IPFS
- Auxiliary tree-based revocation
- Using blockchain to maintain and store cipher text that contains encrypted IPFS URL data along with both revocation list and access policies
- Access control decisions are based on smart contracts
- Providing forward and backward security with only revocation list update
- Existing Cipher text is not actually updated in blockchain, but copy of cipher text is fetched, modified and updated. The updated cipher text copy is always place in blockchain as new transaction for every revoked use

The rest of the paper is structured as follows in the subsequent sections: The section II of this paper explores into an examination of previous studies and related work. Section III describes the proposed Model, providing a in detail explanation. In Section IV, a detailed analysis of the results is presented and discussed. Moving forward, Section V provides insights into future scope and pivotal research directions. Finally, Section VI concludes by summarizing the key findings and implications of our research work.

2. OBJECTIVES OF THE STUDY

1. To protect access policies from infringement.
2. To provide effective revoke mechanisms.
3. For Providing flexible data sharing.

3. RESEARCH METHODOLOGY OF THE STUDY

Systematic approach and techniques are applied to conduct the research and data is collected through different primary and secondary sources.

4. RELATED WORK

This section will focus on most recent research works investigated on the concepts of ABE (Attribute-Based Encryption), ABAC (Attribute-Based Access Control) and blockchain for secure and trustworthy data sharing. Additionally, the section will concentrate on techniques employed for hiding access policies along with various revoking mechanisms employed until now.

The ReLAC method [1] applies the CP-ABE (Ciphertext-Policy Attribute-Based Encryption) mechanism along with an auxiliary binary tree for user revocation. Access policies and revocation are stored as part of the ciphertext. However, to ensure forward and backward security, the ReLAC scheme incurs a high overhead due to the need for cipher text updates and key generation for each revoked user.

The authors in [2] implemented attribute revocation, which indirectly revokes users. However, the overhead of updating secret keys is greater than that of updating the ciphertext.

In [3], the attribute manager was utilized to address the challenge of attribute revocation in the system. However, the scheme incurred additional computation overhead as it required updating the keys and ciphertext of unrevoked users when revoking a malicious user.

During the update phase described by [4], only a single component of the ciphertext related to the user tree was modified. This approach decrease the computational overhead; however, it also resulted in a reduction in the scheme's security.

The CP-ABE scheme proposed by [5] utilizes a binary tree associated with user formation for implementing attribute revocation and user tracing. This scheme has shown to be effective in ensuring security against chosen plaintext attacks and selective access policy scenarios.

In their work, Yang et al. [6] presented a data sharing mechanism that combines blockchain and edge computing to support attribute revocation. However, the scheme mandates the attribute authority to update the attribute key for users who possess the revoked attribute. Additionally, fog nodes are responsible for carrying out ciphertext updates.

Wan et al. [7] proposed a variant of Attribute-Based Encryption (ABE) with user revocation in the random oracle model. However, this approach requires an additional attribute to record expiration time and necessitates re-encryption to uphold data confidentiality against revoked users. As a result, the scheme incurs linear revocation complexity, as the key generation center must distribute updated secret keys to non-revoked users during each revocation epoch.

In their study, Yeh et al. [8] utilized standard Attribute-Based Encryption (ABE) along with a Merkle hash tree to implement user revocation while considering data confidentiality against revoked users. However, they employed a ciphertext re-encryption approach to safeguard data confidentiality, which resulted in a substantial overhead for data owners who needed to re-encrypt their data in each revocation epoch.

In their work, Hoang et al. [9] developed a forward-secure access control mechanism that incorporates attribute revocation. However, in addition to the intricate ciphertext update operations, the scheme also necessitates updating the non-revoked proof and decryption keys for existing users who possess the revoked attribute.

To safeguard users' sensitive information, researchers have explored policy hiding CP-ABE schemes. Nishide et al. [10] introduced the first partially policy hiding CP-ABE scheme, utilizing AND gates and achieving security in the selective model. Lai et al. [11] supported LSSS (Linear Secret Sharing Scheme) policies, achieving full security, although it did not support a large universe. Lewko et al. [12] proposed a CP-ABE scheme, demonstrating its security based on the dual system encryption method [13].

Okamoto et al. [14] successfully developed a scheme that achieves full security. Cui et al. [15] introduced a policy hiding CP-ABE scheme supporting LSSS policies and a large universe, although it only achieves security in the random oracle model. Han et al. [16] proposed a partially policy hiding CP-ABE scheme based on prime order groups, but it relies on a trusted central authority for secret key distribution.

Wang et al. [17] presented a scheme that provided support for revocation and policy hiding but did not accommodate LSSS policies. Moreover, none of the previously mentioned schemes supported outsourced decryption. In contrast, Zhong et al. [18] proposed a CP-ABE scheme that supported outsourced decryption. However, it lacked correctness verification for outsourced results and fell short in protecting user privacy.

In contrast to the pros and cons of the recent works on policy hiding and revocation mechanisms discussed earlier, our proposed method outperforms these existing methods by offering improved performance with reduced computational overhead. Furthermore, our approach includes a blockchain-based access control system, which serves as an additional feature to enhance trust, privacy, and transparency, setting it apart from the aforementioned methods.

5. PROPOSED SECURE DATA MANAGEMENT MODEL (SDMM)

The proposed secure data management model mainly contains three modules:

5.1 Initial setup Module

In this module data owner is going to store his file in decentralized storage IPFS. This module has following steps

- Data owner(O) stores his file in IPFS and will get URL
- Data owner(O) encrypts that URL using CP-ABE
- Encrypted fixed cipher text is associated with updatable access policies written by owner(O) along with updatable empty revocation list
- Now the resulted cipher text is stored in blockchain
- Data owner then deploy four access control smart contracts OAMC (Object Attribute Management Contract), SAMC (Subject Attribute Management Contract), ACC (Access control contract), RMC (revocation Management Contract) to control the access

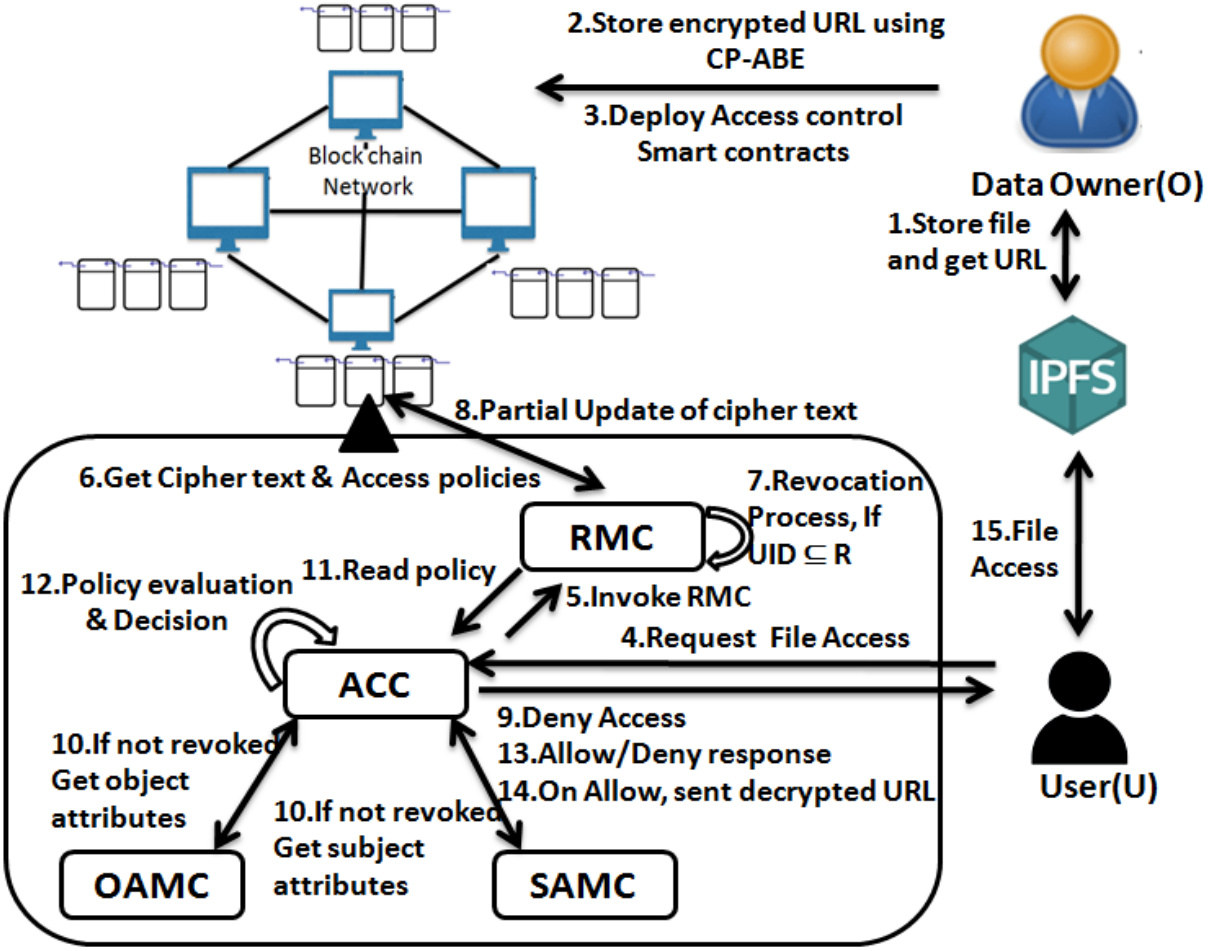
Here OAMC is used to manage attributes related to the object, SAMC is used to manage attributes related to subject, ACC receive requests from user and then it is going to act as PDP (Policy Decision Point) and PEP (Policy Enforcement Point) to make final decisions regarding access, RMC is used to control entire revocation process and also modify updatable components of cipher text such as revocation list and access policies.

5.2 Revocation Module

This module represents the logic that represents sharing and access related aspects. This module has the following steps

- User (U) uses the WebApp and send access request to file Owner (O).
- This request is received by PEP smart contract ACC
- Now PEP forward received access request to PDP which is part of ACC.
- As a Policy Decision Point (PDP), ACC initially invoke RMC.
- Now Revocation Management Contract (RMC) read revocation list(R) and access policies (P) associated with cipher text (CT).
- Now RMC checks whether the user (U) is present in revocation list or not. i.e., if UID $\subseteq$ R
- If user present in revocation list(R), then access request is rejected.
- Otherwise, ACC calls OAMC, SAMC to get object and subject attributes and use access policies (P) to make final access decision.
- If user attributes match access policies(P), then PDP announces decision “Allow” and user(U) is given response with the cipher text that contains URL of file present in IPFS.

FIG. 1: ARCHITECTURE OF SECURE DATA MANAGEMENT MODEL



5.3 Data Sharing Module

This module is used by the file owner (O) to revoke access from User(U). This module has the following steps:

- To revoke access from user(U), data owner sends revocation request along with user id (UID) to ACC.
- This request is received by PEP (Policy Enforcement Point) component of ACC.
- Now ACC invoke RMC (Revocation Management Contract)
- The RMC component invoke the initTree() and updateTree() methods
- Initially initTree() method is invoked to build auxiliary binary Tree(T) out of revocation list(R).
- This binary tree represents all the users who are currently having access to the cipher text of IPFS URL. In this binary tree all the users are represented as leaf nodes.
- After tree initialization, RMC calls updateTree() method to check whether the revocation list(R) contains the UID of the user. Here special algorithms like Cover(R) and Path(i) are used to complete the operation
- If UID $\not\subset$ R, then UID of user is added to revocation list(R) and binary tree is updated to complete revocation process
- Updating revocation list of cipher text represent partial updating, where actual IPFS URL cipher data is fixed
- Now the updated revocation list(R) is updated in the its part of cipher text (CT)
- A special transaction is required to write the updated ciphertext to the blockchain. This is due to the immutable nature of the blockchain, which means that once data is recorded on the blockchain, it cannot be modified or deleted. Therefore, in order to update the ciphertext, a new transaction needs to be created, which includes the revised ciphertext and any associated changes.

The overall architecture that contains aforementioned three models are represented in Fig. 1.

6. EXPERIMENTAL SETUP AND RESULT ANALYSIS

Our model was tested by setting up a local Ethereum blockchain using the Rinkeby testnet. For experimentation purposes, we established this network with ten basic blockchain nodes. The system used for these experiments is equipped with an i5 processor and 16GB of RAM. This configuration ensured that our model could run smoothly and efficiently during testing and evaluation.

We utilized the Ganache software to access the local blockchain network and installed IPFS for decentralized storage. Additionally, we designed a user-friendly WebApp using AngularJS to serve as an interface between users and the blockchain network.

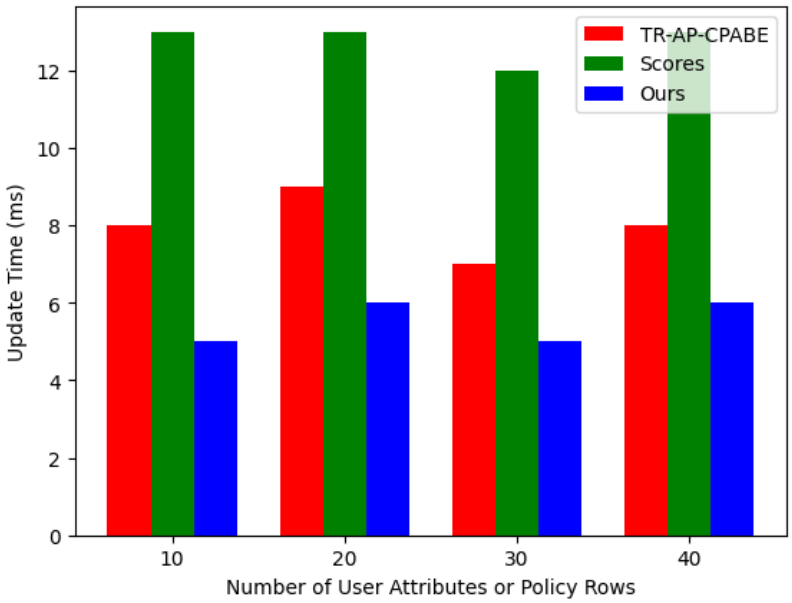
To enable interaction between the WebApp and the blockchain network, we integrated Web3JS within our WebApp, which allows us to communicate with the Metamask extension. Metamask, in turn, facilitates the interaction between our WebApp and the local Ganache blockchain network.

Our secure data management model has been primarily compared to two closely related models, namely the TR-AP-CPABE model [4] and the ReLAC model [1].

6.1 COMPARISON 1: ***Ciphertext updating Time Analysis***

A comparison was conducted among the aforementioned three models regarding the update time of ciphertext, using the metrics of "Number of attributes" and "Update Time." Our model exhibited better performance in this comparison. This is attributed to the fact that our model does not update the existing ciphertext directly in the blockchain. Instead, a modified copy of the ciphertext is created and written into the blockchain as a new transaction.

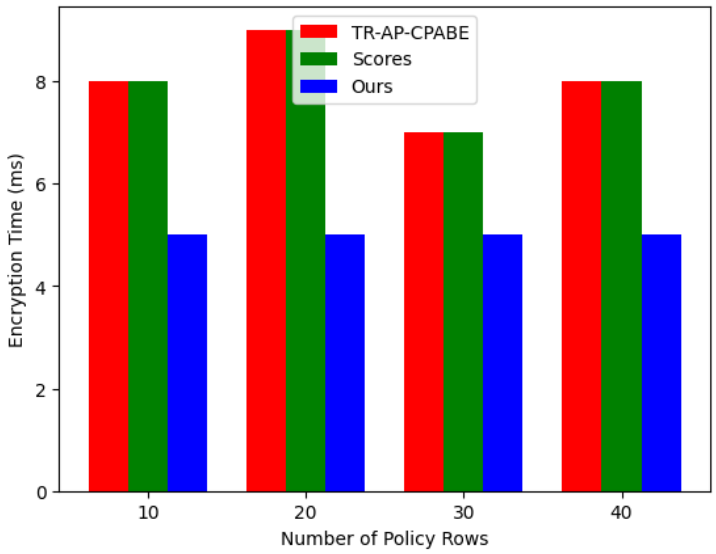
FIG. 2: UPDATE TIME ANALYSIS



6.2 COMPARISON 2: *Encrypt Time Analysis*

In contrast to the TR-AP-CPABE model [4] and the ReLAC model [1], our approach differs in how we handle file encryption. Instead of encrypting the entire file to obtain ciphertext, we store the actual file in IPFS and generate a file URL. This file URL is then encrypted and stored in the blockchain. This approach significantly reduces the time required for encryption compared to the existing models.

FIG. 3: ENCRYPTION TIME ANALYSIS



6.3 COMPARISON 3: *Others*

Our model, implemented in blockchain-based Attribute-Based Access Control (ABAC) with Attribute-Based Encryption (ABE), offers improved trust, privacy, non-repudiation, and decentralization compared to the TR-AP-CPABE model [4] and the ReLAC model [1].

7. FUTURE SCOPE AND RESEARCH DIRECTIONS

Neither the TR-AP-CPABE model [4] nor the ReLAC model [1], including our Secure Data Management Model (SDMM), currently support dynamic access control with temporal dimension and multi-granularity. However, our future goal is to expand our model to encompass both dynamic temporal access control and multi-granularity, incorporating efficient mechanisms for these capabilities.

8. CONCLUSION

In conclusion, our work presents a comprehensive solution for secure sharing of sensitive data by leveraging blockchain technology. We have successfully incorporated Attribute-Based Encrypted (ABE) ciphertext, IPFS file URLs, access policies, and a revocation list within the blockchain framework. By integrating a tree-based revocation mechanism and utilizing Attribute-Based Access Control (ABAC) through smart contracts, such as OAMC, SAMC, ACC, and RMC, we ensure the efficient and seamless execution of necessary operations.

Our system not only secures access policies but also enhances the overall efficiency of the revocation mechanism, enabling effective revocation of access privileges to stop unauthorized usage. Through extensive experimental evaluation and analysis, we have demonstrated the performance of our SDMM when compared to existing approaches.

REFERENCES

1. G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)
2. G. Xiang, B. Li, X. Fu, M. Xia and W. Ke, "An Attribute Revocable CP-ABE Scheme," 2019 Seventh International Conference on Advanced Cloud and Big Data (CBD), Suzhou, China, 2019, pp. 198-203, doi: 10.1109/CBD.2019.00044.
3. S. Wang, K. Guo, and Y. Zhang, “Traceable ciphertextpolicy attribute-based encryption scheme with attribute level user revocation for cloud storage,” PLOS ONE, vol. 13, no. 9, pp. 1–23, 09 2018.
4. D. Han, N. Pan and K. -C. Li, "A Traceable and Revocable Ciphertext-Policy Attribute-based Encryption Scheme Based on Privacy Protection," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 316-327, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2977646.
5. S. Wang, K. Guo, and Y. Zhang, “Traceable ciphertextpolicy attribute-based encryption scheme with attribute level user revocation for cloud storage,” PLOS ONE, vol. 13, no. 9, pp. 1–23, 09 2018
6. Y. Yang, R. Shi, K. Li, Z. Wu, and S. Wang, “Multiple access control scheme for EHRs combining edge computing with smart contracts,” Future Gener. Comput. Syst., vol. 129, pp. 453–463, 2022.
7. Z. Wan, J-. Liu, and R. H. Deng, “HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 743– 754, Apr. 2012.
8. L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, “Cloudbased fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation,” IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 532–544, 2018
9. V. Hoang, E. Lehtihet, and Y. Ghamri-Doudane, “Forward-secure data outsourcing based on revocable attribute-based encryption,” in 15th International Wireless Communications & Mobile Computing Conference, IWCMC 2019, Tangier, Morocco, June 24-28, 2019. IEEE, 2019, pp. 1839–1846.
10. S. Tu, F. Huang, S. Zhang, A. Badshah, H. Alasmary, and M. Waqas, “Ciphertext-policy attribute-based encryption for securing IoT devices in fog computing,” in International Conference on Computer, Information and Telecommunication Systems, CITS 2022, Piraeus, Greece, July 13- 15, 2022, G. A. Tsihrintzis, M. Virvou, K. Hsiao, P. Nicopolitidis, and Y. Guo, Eds. IEEE, 2022, pp. 1–7.
11. R. Sarma, C. K. Chaudhary, and F. A. Barbhuiya, “PAC-FIT: an efficient privacy preserving access control scheme for fog-enabled IoT,” Sustain. Comput. Informatics Syst., vol. 30, p. 100527, 2021.
12. C. K. Chaudhary, R. Sarma, and F. A. Barbhuiya, “Rma-cpabe: A multiauthority cpabe scheme with reduced ciphertext size for IoT devices,” Future Generation Computer Systems, vol. 138, pp. 226–242, 2023.
13. S. A. Khowaja, P. Khuwaja, K. Dev, I. Lee, W. U. Khan, W. Wang, N. M. F. Qureshi, and M. Magarini, “A secure data sharing scheme in community segmented vehicular social networks for 6G,” IEEE Trans. Ind. Informatics, vol. 19, no. 1, pp. 890–899, 2023.
14. Y. Lin, X. Wang, H. Ma, L. Wang, F. Hao, and Z. Cai, “An efficient approach to sharing edge knowledge in 5g-enabled industrial internet of things,” IEEE Trans. Ind. Informatics, vol. 19, no. 1, pp. 930–939, 2023.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue, as well as on the journal as a whole, on our e-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our e-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward to an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals