Vol. 01, Iss. 2 (2024) 86-94, DOI: 10.61552/JSI.2024.02.005

Journal of Sustainable Development Innovations

www.jsi.aspur.rs

A Hybrid Key Management Approach for Enhancing Data Sharing Security with Insider Threat Detection

S. Hrushikesava Raju[a,b,*], U. Sesadri[b], S. Thulasi Krishna[c], K. Selvam[a], V. Balaji[e], Gunikhan Sonowal[f]

[a]*Department of Computer science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram Guntur, Andhra Pradesh – 522302, India,*
[b]*Vardhaman College of Engineering,Kacharam, Shamshabad Road,Hyderabad, Telangana, 501218, India,*
[c]*Department of CSE, Sree Rama Engineering College, Tirupati, India,*
[e]*School of Technology, GITAM University, Nagadenehali, Doddaballapur taluk, Bengaluru, Karnataka, 561203, India,*
[f]*Assam down town University, Sankar Madhab Path , Gandhi Nagar, Panikhaiti, Guwahati, Assam, India.*

Keywords:

Cloud computing, misbehavior detection, data integrity, novel key management technique, timely alerting, performance, and accuracy.

* Corresponding author:

S. Hrushikesava Raju
E-mail: hkesavaraju@gmail.com

Received: 5 April 2024
Revised: 16 May 2024
Accepted: 19 June 2024

A B S T R A C T

The secure sharing of group data in cloud environments poses challenges, particularly when attempting to identify individuals engaging in fraudulent behaviors. While existing studies have touched upon this issue, this research introduces a novel key management strategy that prioritizes crucial features such as performance, accuracy, and trustworthiness. In the context of cloud data sharing, several key points are considered, including the precise assignment of privileges to groups, the tracking of reports containing sensitive user information, the monitoring of user or group misconduct using an innovative key management technique, and timely alerting of the cloud owner. The proposed novel key management technique adopts a level-wise authorization process, diligently recording all actions based on the rights assigned to perform specific tasks. Performance, accuracy, and trustworthiness metrics are then evaluated against a set of well-defined strategies, and the results are effectively visualized. The efficiency of this approach is assessed and visualized in results. This ensures the approach's robustness and suitability for various cloud environments. By addressing the challenges associated with identifying misbehaving attitudes in cloud settings, an efficient and trustworthy key management system is ensured. The proposed approach enhances data security and the integrity of information sharing in the cloud, benefiting individual users and businesses alike. Ultimately, this innovative solution contributes to creating a safer and more reliable cloud computing environment, fostering seamless collaboration and information sharing among users while safeguarding their valuable data.

1. INTRODUCTION

In the cloud environment, providing security is a challenging task although there are many techniques and approaches are existed. In the public clouds, groups are available and communication among them misleading their rights they possess at rare times. In such cases, to trace where the misleading behavior is occurred and tampered the principle of security. In groups, there are few might leak the information of the context to others which cause huge loss or damage to the organization. There are many studies and methodologies existed to handle these kinds of scenarios. In group, the security is maintained using terms such as accumulated conference key, stating the sender and recipient of the information. Data sharing from the group to other who is authenticated in the organization, must get the copy of the piece which was shared by someone from the group. To guarantee the security of information, members of the group are responsible. Storing data in a cloud is one-way a challenging, and need to protect such piece of data is another challenging. Many barriers like online availability of data, fast accessing, sharing data in a group or from one to other are eliminated using the establishment of cloud computing. Not only these are to be achieved, but also many trending benefits like backup and restore, and security aspects. The issues are classified as certain categories.

a) Category1: Abilities support such as static or dynamic.
b) Category2: Transparent scheme while sharing.
c) Category3: Confidentiality maintenance.
d) Category4: Traceability support when bane occurs.
e) Category5: Fault tolerance.
f) Category6: Policy Updating whenever required.
g) Category7: Alerting the Actions when members transferred or inactive.

The issues raised and addressed in the above mentioned categories are all to be rectified using cloud computing. Cloud computing is the latest trending in the competitive business applications. Every industry is preferring the cloud to manage their activities, in order to store their details.

The category1 related issues classified as traditional and dynamic in which traditional resembles static whereas dynamic specifies changing the patterns would also be supported by the existing environment. The category2 issues include the anonymous users would enter into the cloud are stopped using groups, only members of the organization would access the resources, every log of the activity is stored in daily report, and alerting the report to the admin of the group. The sorting of all these are to be taken care using policies. The category3 issues include activities imposed to maintain confidentiality of a group. It is typical to identify the member who is misbehaving but acting like genuine. In the course of activities, if activity is damaging the survival of the group's data, must take action against such members. The category4 issues include identifying the user who tampered policy of the group and the system. The conference key distributed while sharing of the data.The category 5 issues include the group to be consistent by imposing dynamic policies when required and should with-stand in case of mismanagement through appropriate actions.The category6 issues include rules are framed as a policy, which should be obeyed by the system. Based on changes happening over the time, a new rule to be defined or modifying the current rule in a policy to be supported and encouraged. The category7 issues include misbehaving members, their log activities to be monitored, inactive members monitoring, and members diverting confidentiality are noted and appropriate actions are imposed in order to maintain loss free environment. To overcome all these issues, defining a dynamic policy as well as member level-wise forming of conference key plays a key role. In this, first is policy framing before starting a group, which should be dynamic to include new rules and should allow existing rules to be refined according to the specific features. The second is conference key validation by level-wise member scrutiny. It is necessary because members should be transparently showcase who is initiated the request for sharing and who is the recipient to receive while sharing. The transparency and policy re-framing are top priority services maintained by the novel approach.

2. RELATED WORK

In this, what studies involved in providing the confidentiality as well as security over the public cloud system. The below table summarize the studies and their themes.

Table 1. Significant Studies on Cloud computing for sharing of the data.

Reference No., Year and authors	Theme	Methodology used	Parameters on which study assessed
[3], 2018, Jian Shenat el	Sharing of data in the public clouds	Group signature and common conference key	Security
[4], 2017, S. Hiremath at el	Data privacy and integrity	Auditing technique using TPA	Verification of audit files
[5], 2017, H. Guesmi	Identity based cryptography	Securely storing data using IBE	Privacy and Security
[6], 2021, A. Kumar	DNA cryptography, HMAC technique and TPA	Encoding and decoding phase, verifies the HMAC value	Security
[7], 2014, R.Raampriya	Auditing and Logging system	Controlling the user and activities are based on Logging and Auditing	Accessing
[9], 2020, Xiuqing Lu at el	Secure sharing scheme	Security provided in phases and achievement of light weight computations.	Security
[13], 2019, Junfeng Tian at el	Group member and audit agent involved in providing the security using specific strategies.	Providing security over data using TCP sliding window and audit agent privileges.	Security

As per [1], focusing on the efficiency in sharing data from a group by any anonymous user. The security is maintaining using encryption techniques and group signature. Providing security over multiple owners on the dynamic groups is a challenging task, which somehow addressed but still chances would be there not to trace the identify. In the aspect of [2], the depicted work focuses on security while sharing of data. The owner of the group would alert the access key as well as specific time bound to access the resources available in the cloud. The cloud nature may not be dynamic, leads to mislead the member's nature. In the view of [3], the key terms such as group signature and common conference key are used to provide security over the group to share the data. Supporting of anonymous users is the pitfall of this work and approach defined for the tracing of the misleading member is not much effective. In the junction of [4], the factors time and spending investment are minimized when cloud computing is used and leads to validate integrity check using efficient auditing technique with the help of third party auditing. The security is provided using AES and SHA-2. The significant taking factor is on auditing different files that would consume constant time. From the view of [5], the data stored in plain text may not guaranty security and scope for threats. In order to store the data in a cloud using identity based cryptography preserves storage. It focuses on privacy and security imposed on the cloud using the proposed policy. As reference to [6], the security is provided using three techniques such as DNA cryptography, HMAC, and TPA. These techniques applied one after the other fashion to provide security. At the time of encoding, HMAC value computed and stored on the cloud. At the time of decoding, the HMAC value is generated by TPA matches, then accessing and further privileges are supported. From the study [7], the uploading is done in JAR form. The activities of the shared member of a cloud are monitored using logging system as well as auditing mechanism. These approaches provide control over the users who are involved in sharing the data. In the view of [8], demonstration of terms related to cloud computing is done. The regulatory proposed over old technologies used in the cloud are mentioned as well as mentioned the ways how to protect the sensitive data. The issues over the cloud are discussed. As per [9], the data owners and Data requesters computation made light operations when shared data over

a cloud might experience few challenges atthe mobile terminals such as privacy and security. To sort such related issues would be solved using secure sharing scheme which works in phases in which first phase verifies authorization and second phase verifies integrity followed by achieving of lightweight operations. The objective of [10], the SeDaSC proposes novel scheme that obeys five important factors such as privacy, access, sharing, insider threat security, and forward and backward accessing. The performance and assessment of this approach is scrutinized by few pre-defined libraries and their results are compared. The work of [11], it provides dynamic policies to update the passwords based on the frequency of users. A novel algorithm designed that provides password according to the dynamic policies at the time of password setting. In regard of [12], the cryptographic server is the component that plays key role which serves as key validator based on functionalities and encryption standards. Here, the key is composed of two fragments in which one is ACL and is part of the key, and second is attached to the key while transmitting the data. This way it provides few cloud approaches as combination called hybrid approach. From the aspect of [13], the computations involved in the group members are complex and are made light using auditing agent, few specific strategies such as third party medium approach. The security is preserved using TCP sliding window concept as well as auditing agent privileges. From aspect of [14], the attacks raised when sharing data among the clouds such as collusion attacks need to be minimized. The group key management protocol ensures the mixed encryption over the data to be secured. As reference from [15], the privacy provided over the shared data using strategies such as data service provider, computation party, and flexibility control to be achieved using homomorphism attribute based encryption. From [16], the attribute based encryption with integration of anonymise access policy and signature scheme helps to identify the insider of cloud who modifies the data by decrypting and again encrypting, that cause adverse effect on the privacy. In the view of [17], the issues related to privacy and security are addressed and concluded how to overcome such issues over the cloud computing. The provider have certain privileges and users would make use of services of the cloud. When sharing the data over the cloud, some issues to be resolved by certain strategies and approaches. As per [18], the ASP based on AKU policy supports common operations over the cloud along with revocation scheme. The guarantees the fake users not to enter into the cloud. As related to [19], it reviewed few studies such as cloud cube model, Multiple tenancy model, Multi clouds database model, Risk accumulation model. These distributed models are evaluated based on certain factors and are summarized. From the pint of [20], the IBEET-DBA scheme make use of equality tests which could be taken care by cloud server and date-stamped authorization used to validate the cipher texts for authenticated users. The security is provided by using both the mentioned components while sharing the data. As per [21], the approach CSSM defined with integrated features such as dispersion, distributed storage, and hierarchical management helps to share in less time although huge data to share, and achieves security over the data.

The studies mentioned in this are dealing issues over the cloud such as security, privacy, and other features. The motto of this study is cloud is of dynamic nature means members joining and leaving the group is in flexible with enhanced security. The tracing of the member who is insider would be caught if behaves wrongly. The proposed study focuses on traceability and security over the data sharing in the cloud.

3. PROPOSED METHODOLOGY

The types of problems discussed in the introduction would be listed in the below table along with that necessary action or factor to provide.

In most of these cases, incremental key, auditing daily basis using cloud server and administrator are used in sorting out the issue. The proposed system's work is composed into four modules.

Table 2. Issues identification as per category.

S.No.	Problem Category	Solution or Factor to be deal in such case
1	Category1: Abilities support such as static or dynamic	Group nature should be dynamic in sense members could leave and new members could join, may effect group signature
2	Category2: Transparent scheme while sharing	Member wise would contribute in generating the conference key and is incremental
3	Category3: Confidentiality maintenance	Outsiders won't be allowed to read or interpret the information without all members generated incremental key
4	Category4: Traceability support when bane occurs	Logs are preserved to trace the bane and auditing would be done daily basis to eradicate such bane issues
5	Category5: Fault tolerance	It also addressed with the cloud service provider
6	Category6: Policy Updating whenever required	The administrator of the group based on organization requirements, would update the policies.
7	Category7: Alerting the Actions when members transferred or inactive	Joining and Exiting the members of the group, would be taken care by administrator. Exit members account to be removed and new members accounts to be added.

3.1 Encryption and Decryption

The purpose of encryption is to convert the original source into unknown text whereas decryption is cyper text(encrypted text) to be converted into original text. During this process, keys are used. The key should be unable to be predicted by the hacker or attacker.

The following diagram shows the flow of these key term's working:

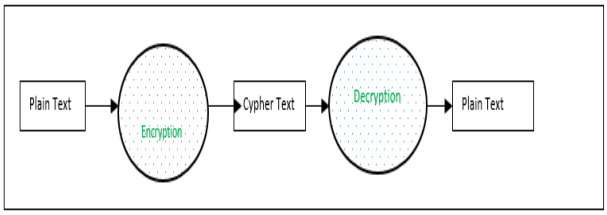

Fig. 1. Encryption and Decryption techniques.

Pseudo_Procesure

Encryption(Msg,sender,receiver):

Step1: If receiver is authenticated, send Msg easily using sharing. While sharing, default cloud encryption technique is applied. The default scheme used is AES-256.

Step2: If receiver is outside of present cloud, must be transparent to the group, call the auto_incremental_key_scheme().

Step3: The receiver consists of private key provided by the encryption algorithm and should be validated by incremental accumulated key.

Step4: Read the source text

3.2 Auto Incremental key scheme

The purpose of introducing this is to make working as transparent in the sense all the members of the dynamic group must know who is new member added and who is old user left. The privileges also provided for new user and disenabled for old user who left the organization. The groups are maintained in any organization as per their designations. Some information might share easily to the other groups but some information to be maintained confidentially at the high level must be secret.For such groups, members must be limited like 5 or 10 or 15 or 20 or 30 and should be less than one threshold value. For example, assume group size is 10. In such a case, each member of the group must possess a dynamic key as OTP which could be delivered to their registered mail and by SMS. If all members of the group would enter their OTP, then final key would be reframed to match to its originator key. Then only, information is to be shared. During this scenario, which groups or members of the cloud retrieved the information would be stored in logs. This scheme designed provides most security and administrator would have right to modify the members and their privileges.

Pseudo_Procedure

Auto_incremental_key_scheme(N,ΔK):
Input: Group Size(N), Dynamic OTP Part as ΔK
Output: Incremental_key

Step1: for i=1 to N do
ΔK=random()
Alert("SMS to the"+i+"th member"+ΔK)
Incremental_key+=ΔK

Step2: The Incremental_key value is alerted to group admin and automatic dispense to the receiver after successfully verifying the authentication.

2.1 If receiver credentials to be verified such as username and password from the cloud service provider, need to enter the Incremental_key for reading the Msg.

2.2 Accessing is allowed

Step3: call log_auditing()

Step4: Generate report

3.3 Log Auditing

Every user activity is recorded and stored in logs. These logs are maintained at central cloud server which posts them to the organization president or chairman as a backup. The benefit of logging is misconduct of the member is notified to the higher levels.

Pseudo_Procedure

Log_Auditing(Privileges,N):

Step1: for specific member □ Group,

Validate the member privileges ie

If(Member(privilege)□ Σprivileges)

Need not alert

else

Alert the violation and store in log

Step2: Report= Σ violated activity as a log record

Step3: Cloud Server as well as Group administrator would recommend actions according to the logs

3.4 Reporting for each update

At the end of each day or each week as per customization of administrator, the reports are generated and sent to organization's mail as a backup.

Pseudo_Procedure Update_report(choice):

Step1: if(choice==1)

Send report Day-wise

else if(choice==2)

Send report week-wise

Step2: In additional to alerts on violation, these consolidated reports also communicated to the concerned.

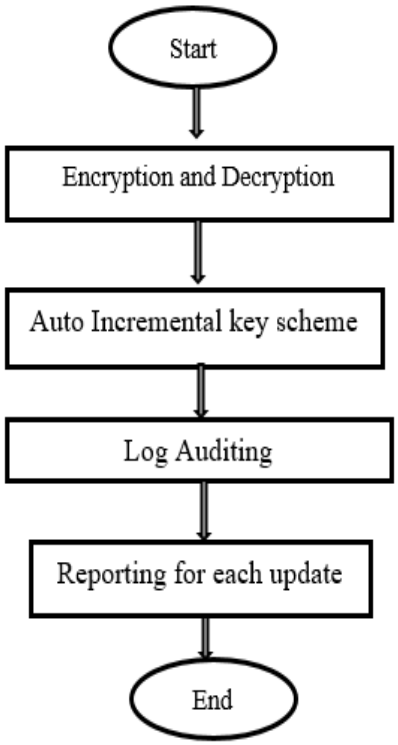

Fig. 2. Modules of the Hybrid Key Management System ensuring transparency and security.

The proposed system with its significant modules auto_incremental_key_scheme(), and log_auditing() plays a crucial role than the encryption,decryption, and generation of report. The auto_incremental_ key_scheme() ensures transparency and security whereas log_auditing() ensures both traceability of member's misconduct and security for the group information.

4. RESULTS

The evolution of security when sharing from the group is completed analyzed with few metrics such as Activities transparent to group, traceability in case of misconduct using logs auditing, and security is the top defensive factor observed and provided.

The below table shows the factors that contributed to the benefit of their models and are analyzed here:

4.1 Traceability: It represents the member possessing the misconduct identification. It uses auditing and logging feature.

Table 3. Models with traceability feature.

S.No.	Model	Factor	% of Focus
1	Hybrid key management scheme	Incremental_key and logs	100
2	DNA cryptography	DNA	98
3	Auditing and Logging system	Logs	99
4	Light Weight Computation Model	Less resources	80

4.2 Transparent

It represents to whom the information shared to be known to every member of the group. It uses incremental_key_scheme().

Table 4. Models with transparent feature.

S.No.	Model	% of Focus
1	Hybrid key management scheme	100
2	DNA cryptography	95
3	Auditing and Logging system	99
4	Light Weight Computation Model	70

4.3 Security

It uses by default AES for encryption and decryption and also uses incremental_key field at the receiver side. The administrator may be cloud server with defined policy.

Table 5. Models with security feature.

S.No.	Model	% of Focus
1	Hybrid key management scheme	100
2	DNA cryptography	99
3	Auditing and Logging system	99
4	Light Weight Computation Model	80

The following graph, would showcase the efficiency of the models in which proposed approach proved better performance.

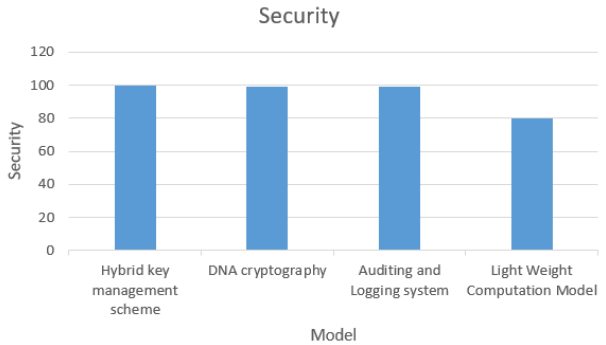

Fig. 3. Security evaluation over significant studies

4.4 Performance

It uses simple operations only while working instead of creating overhead for each few specific activities.

Table 6. Models with performance feature.

S.No.	Model	% of Focus
1	Hybrid key management scheme	100
2	DNA cryptography	90
3	Auditing and Logging system	90
4	Light Weight Computation Model	95

The working computation is easily taken up without involving additional overhead in case of our proposed approach and is demonstrated as below:

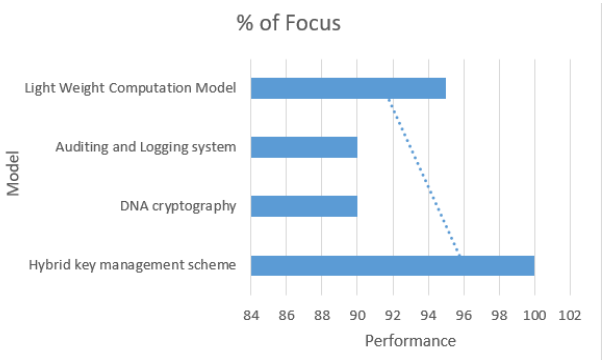

Fig. 4. Performance evaluation over significant studies.

5. CONCLUSION

Sharing of messages, information, data out of a group to any other should be transparent so that risks are minimized and leads to be healthy group. Not only this, traceability if any group member would like to misbehave, other members might know immediately. In addition, security is top notch factor that preserves and protects the data and won't share to any third party without your knowledge. The security to be obtained using incremental key that is framed after all members provides their dynamic OTPs. Each member knows the sender initiated and receiver who gets the data. The most significant factors are security and performance in which security is addresses using incremental key update and log auditing. The other is processing involves less overhead in this scenario because of efficient handling methodologies and supportive dynamic environments.

Acknowledgement

I would like to thank my co-authors who gave inputs and transformed into efficient work.

REFERENCES

[1] P. N., J. B. R., D. B. S., and V. B. G., "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in The Cloud," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 2, no. 13, NCRTS 2014, 2014.

[2] S. Uthayashangar, P. Dhamini, M. Mahalakshmi, and V. Mangayarkarasi, "Efficient Group Data Sharing In Cloud Environment Using Honey Encryption," in *Proc. IEEE Int. Conf. System, Computation, Automation and Networking (ICSCAN)*, 2019, pp. 1-3, doi: 10.1109/ICSCAN.2019.8878759.

[3] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 912-925, Apr. 2018, doi: 10.1109/TIFS.2017.2774439.

[4] S. Hiremath and S. Kunte, "A novel data auditing approach to achieve data privacy and data integrity in cloud computing," in *Proc. Int. Conf. Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEEECCOT)*, 2017, pp. 306-310, doi: 10.1109/ICEECCOT.2017.8284517.

[5] H. Guesmi and L. A. Saïdane, "Improved Data Storage Confidentiality in Cloud Computing Using Identity-Based Cryptography," in *Proc. 25th Int. Conf. Systems Engineering (ICSEng)*, 2017, pp. 324-330, doi: 10.1109/ICSEng.2017.32.

[6] A. Kumar, "Framework for Data Security Using DNA Cryptography and HMAC Technique in Cloud Computing," in *Proc. Second Int. Conf. Electronics and Sustainable Communication Systems (ICESC)*, 2021, pp. 898-903, doi: 10.1109/ICESC51422.2021.9532950.

[7] R. Raampriya and L. Vinothini, "Accountable Data Sharing in Cloud Using Logging Mechanism," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 2, no. 01, IFET 2014, 2014.

[8] J. Sen, "Security and Privacy Privacy Issues in Cloud Computing," *arXiv*, 2013, [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf.

[9] X. Lu, Z. Pan, and H. Xian, "An efficient and secure data sharing scheme for mobile devices in cloud computing," *J. Cloud Comput.*, vol. 9, no. 1, p. 60, 2020, doi: 10.1186/s13677-020-00207-5.

[10] M. Ali, R. Dhamotharan, E. Khan, and A. Zomaya, "SeDaSC: Secure data sharing in clouds," *IEEE Syst. J.*, vol. 11, no. 2, pp. 1-10, Jan. 2015, doi: 10.1109/JSYST.2014.2379646.

[11] A. Singh and S. Raj, "Securing password using dynamic password policy generator algorithm," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1357-1361, 2022, doi: 10.1016/j.jksuci.2019.06.006.

[12] G. G., K. S. V. Vamsi, Y. S. Subhash Reddy, et al., "A Hybrid Scheme in Cloud Computing for Secure Sharing of Data in the Cloud," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 2S11, Sep. 2019, ISSN: 2277-3878.

[13] J. Tian and X. Jing, "A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage," *IEEE Access*, vol. 7, pp. 68071-68082, 2019, doi: 10.1109/ACCESS.2019.2916889.

[14] S. Zhang, S. Han, and B. Zheng, "Group Key Management Protocol for File Sharing on Cloud Storage," *IEEE Access*, vol. PP, no. 99, pp. 1-1, Jan. 2020, doi: 10.1109/ACCESS.2019.2963782.

[15] W. Ding, Z. Yan, R. H. Deng, et al., "Privacy-Preserving Data Processing with Flexible Access Control," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 363–376, Mar.–Apr. 2020, doi: 10.1109/TDSC.2017.2786247.

[16] S. Sabitha and M. S. Rajasree, "Access control based privacy preserving secure data sharing with hidden access policies in cloud," *J. Systems Archit.*, vol. 75, no. C, pp. 50–58, Apr. 2017, doi: 10.1016/j.sysarc.2017.03.002.

[17] E. Abu Shanab, "Addressing Security and Privacy Issues in Cloud Computing," *J. Emerg. Technol. Web Intell.*, vol. 6, no. 2, May 2014, [Online]. Available: https://www.academia.edu/33450383/Addressing_Security_and_Privacy_Issues_in_Cloud_Computing.

[18] S. Nandan Kumar, "ASP: Advanced Security Protocol for Security and Privacy in Cloud Computing," *Am. J. Inf. Syst.*, vol. 4, no. 2, pp. 17-31, 2016, [Online]. Available: https://www.academia.edu/23407546/ASP_Advanced_Security_Protocol_for_Security_and_Privacy_in_Cloud_Computing.

[19] A. Prasanth, "Cloud Computing: Secure and Scalable Data Access Security Models," *Int. J. Comput. Appl.*, vol. 170, no. 4, Jul. 2017, [Online]. Available: https://www.ijcaonline.org/archives/volume170/number4/prasanth-2017-ijca-915084.pdf.

[20] X. J. Lin, Q. H. Wang, L. Sun, and H. P. Qu, "Identity-Based Encryption with Equality Test and Datestamp-Based Authorization Mechanism," [Online]. Available: https://www.researchgate.net/publication/349118930_Identity-Based_Encryption_with_Equality_Test_and_Datestamp-Based_Authorization_Mechanism.

[21] H. Song, J. Li, and H. Li, "A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption," *IEEE Access*, vol. 9, pp. 63745-63751, Jan. 2021, doi: 10.1109/ACCESS.2021.3075340.

[22] S. H. Raju, L. R. Burra, S. F. Waris, and S. Kavitha, "IoT as a health guide tool," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 4, 2020, doi: 10.1088/1757-899X/981/4/042015.

[23] S. H. Raju, L. R. Burra, A. Koujalagi, S. F. Waris, "Tourism enhancer app: user-friendliness of a map with relevant features," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022067.

[24] S. H. Raju, L. R. Burra, S. F. Waris, and S. Kavitha, "IoT as a health guide tool," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 4, 2020, doi: 10.1088/1757-899X/981/4/042015.

[25] S. H. Raju, L. R. Burra, A. Koujalagi, S. F. Waris, "Tourism enhancer app: user-friendliness of a map with relevant features," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022067.

[26] S. S. R. Jasti, V. Revanth, K. D. N. Rammohan Chowdary, K. C. S. V. Charan, S. H. Raju, and S. Kavitha, "Crop Intelligent: Weather based Crop Selection using Machine Learning," in *Proc. Int. Conf. Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, 2023, pp. 1594-1600, doi: 10.1109/ICSCDS56580.2023.10104898.

[27] S. Hrushikesava Raju, S. Thrilok, K. P. S. K. Reddy, G. Karthikeya, and M. T. Kumar, "An IoT Vision for Dietary Monitoring System and for Health Recommendations," in *Inventive Communication and Computational Technologies*, G. Ranganathan, X. Fernando, and F. Shi, Eds., Lecture Notes in Networks and Systems, vol. 311. Springer, Singapore, 2022, pp. 865-873, doi: 10.1007/978-981-16-5529-6_65.

[28] S. Hrushikesava Raju, V. Lakshmi Lalitha, P. Tumuluru, N. Sunanda, S. Kavitha, and S. F. Waris, "Output-Oriented Multi-Pane Mail Booster," in *Smart Computing and Self-Adaptive Systems*, CRC Press, 2021, pp. 48-57, doi: 10.1201/9781003156123-4.

[29] S. Hrushikesava Raju, L. R. Burra, S. F. Waris, V. Lakshmi Lalitha, S. Dorababu, and S. Kavitha, "Eyesight Test through Remote Virtual Doctor Using IoT," in *Smart Computing and Self-Adaptive Systems*, CRC Press, 2021, pp. 59-69, doi: 10.1201/9781003156123-5.