International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228641

A Framework for Data Security and Sharing in Cloud Computing Environments by Using Cryptographic Algorithms

Dr. Rafath Samrin[1], Aluri Gopi[2], Mangalampalli Sesha Sai Lakshmi Lavanya[3], K Swetha[4]

[1]Associate Professor, Department of CSE (AI & ML), CMR Technical Campus, Hyderabad, Telangana, India

[2]Assistant Professor, Department of Electronic & Communication Engineering, CMR Engineering College, Hyderabad, Telangana, India

[3]Assistant Professor, Department of CSE (DS), CMR Engineering College, Hyderabad, Telangana, India

[4]Assistant Professor, CSE (Cyber Security) Department, Sri Indu College of Engineering and Technology, Hyderabad, Telangana, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 314-322

Article History
Accepted: 12 Nov 2022
Published: 28 Nov 2022

ABSTRACT

Cloud storage is a liberating cloud application group to establish an internal database system. However, cloud storage raises security concerns. Inside the case of data sharing, the data is both cloud-specific and ancient music. Secure data distribution within a group which prevents the examiner from fearing legitimate but cruel agents important research questions. Data sharing and cloud storage play an important role in communication, as they can provide users with efficient and effective security services. To protect shared secret data, cryptographic methods are often applied. A large number of researchers, universities, government departments and commercial companies are adopting the cloud environment due to the initial investment, its high scalability and its many features. Despite many initiatives supporting the cloud environment, it faces many challenges. Data protection is a major concern in the information security and cloud computing industry. Many solutions have been developed to overcome this challenge. However, there is a there is not enough research between the current solutions and the emerging need to analyze, organize and analyze the important work that is done to study these solutions to respond to the field. This article provides an overview of research and process analysis, as well as an in-depth analysis of the topic of distributed security and data storage in cloud environments. Discussions on each dedicated process include: data protection services, rights and changes in the field, basic and comprehensive information including scope of work, achievements, limitations, future directions, etc. in any solution. In addition, a comprehensive and comparative analysis of these current methods is discussed. Then, the speed of the process is measured by the requirements of the search space and the future directions in the field are shown. The authors agree with this report. These plans will be what motivates researchers to do research in the field.

Keywords : Cloud Computing, Privacy, Security, Data Protection, Machine Learning, Cryptography, Watermarking, Access Control.

I. INTRODUCTION

As attractive and desirable in terms of value, the development and implementation of cloud-based applications has seen a significant increase in companies and the research community in recent years. Cloud storage is one of the most successful cloud-based applications as it meets the growing need for efficient data sharing. Sharing big data with many data sharers is a very expensive activity, the cost to the data owner is usually the number of data sharers. Although this cost can be reduced in shared data size by using cloud storage. All the data sharer needs to do is upload the data to the cloud and grant access to the data sharer. After that, the data distributors can access the cloud data instead of being the data owner. Despite the benefits of data sharing and cloud storage, it also provides many opportunities for an adversary to gain unauthorized access to shared data.

To protect the privacy of shared data, cryptographic schemes are often implemented. The security of the cryptographic scheme is achieved by the security of the underlying secret key. Currently, private keys are stored on computers in many existing encryption schemes. Although it has been reported that some viruses can reveal encrypted keys. To solve the key disclosure problem, many methods have been proposed, such as remote public key systems and public key systems. Data is identified as a great value of the organization Because it describes different parts of any company. This is the main point of knowledge, information, Finally, wisdom for good judgment is good and morally. It may be to help cure an illness, increase business income, make a home more efficient or have a job to achieve its objectives and improve its performance [1]. In addition, data storage, analysis and sharing are an important function of any organization that needs to be improved its performance [2]. However, the explosive evolution data, high-pressure work and industry storing large amounts of data locally [3]. Also, it became it is difficult to analyze the data due to the high cost [4].

Many companies have moved to the cloud for these services due to many benefits such as on-demand services, scalability, reliability, elasticity, scale of work, disasters recovery, availability and many others [5]. cloud computing is a paradise that allows for ample security opportunities and mathematical ability and finance. It gives users access services provided on multiple platforms, independently whose place and time therefore give much convenience for cloud users [6]. By moving Local data management system and cloud storage and usage cloud-based services, users can save money and Improved functionality to manage operations and setup cooperation [7]. Therefore, individuals and organizations turning to the cloud for most of their work [8].

Cloud expansion is also accelerating technology, it is not possible to imagine that it is almost all business will move to the cloud for the foreseeable future future [9]. Despite the many features offered by the cloud, it encounters many obstacles that can hinder it rapid growth, if not properly treated [10]. consider this in fact the implementation, when the company allows its employees or domain to store and share data through the cloud. By using the cloud, the business can be completely Released the burden of storing and storing things regional data [11], [12]. However, it also becomes different security fear, which is the main concern of the cloud users [13]. First, remove the data from the cloud Subscribers and data are above the users' score and user discomfort because the data generated may understand sensitive and useful information.

Secondly, Data distribution is implemented in hostile environments and open environment, and the cloud becomes a an insult. In the worst case, user data can The cloud server will be exposed for illegal profit [14], [15]. In addition, data will be shared between different important people, such as business partners, employees, customers, etc., inside or outside the organization camp to improve business performance. However, this data may be corrupted by the receiver intentionally or unintentionally disclosed to unauthorized persons others [12].

In addition, cloud data is shared Many jobs seem to have different needs than benefits objective. However, the receiving party may disclose the data when he received it. Data can be disclosed by affected parties or steal it from unauthorized persons through illegal means to get. Loss or loss of data can be catastrophic organizational secrets. This can reduce the value of shareholders, reject company-level advertising and destroy goodwill and company reputation [18]. Like data is an important part of the organization, so it is important to protect this property. It seems important to find a solution that can effectively protect data when sharing environment.

Many types of data storage in cloud environments has been researched and developed for many applications. Data security is often accessed through leaks prevention and detection of leaks in this topic is focused on and achieve effective protection by preventing leakage and find the cause of the disturbance Shown in Figure 2. Ways to intercept data Leaks are reproduced using encryption, access control different techniques and algorithms in machine learning while leak detection is mainly done by watermark in the process of probability. It is reported that 83% of the administrative burden moved to the cloud platform by 2020, bringing 90% within one year from 2021 [9]. cloud computing Business is expected to grow at a rate of 14:6% The annual growth rate would be a $300 billion industry by 2022 compared to 188 billion dollars in 2018 [2]. In addition, There will be 75 billion connected IoT devices 2025, that is an increase by 3 compared to 2019.

IoT is the future and everything will continue to be different connected through technology using cloud services [2]. Plan to get the cloud to share the required data Cloud computing has greatly reduced data management cost as it increases flexibility and storage capacity [3], [4]. Despite this, it is also good serious risks in data protection [5]. Specifically, Cloud users cannot fully trust cloud services Providers (CSP) like managing data stored in the cloud can be private and sensitive [6]. Also, data owners have serious concerns when sharing data in the cloud due to the inevitable loss of data control opening the way for unauthorized access to data [7]. Therefore, security and privacy of sensitive data has become a major issue concerns of cloud users when using the cloud
work.

II. RELATED WORK

Xu et al. [9] proxy returns undocumented policy (CL-PRE) scheme for sharing stored data within groups in the clouds. In the CL-PRE scheme, the data owner encrypt data with a symmetric key. Finally, the people the symmetric key is encrypted with the public key of the data the owner. Encrypted data is uploaded to the key the cloud. Another hidden key (which happens such as proxy re-encryption) which becomes decryptable by the user's private key.

Do not share the public key with the plan is not based on certification. Employees Identity is used to generate public and private keys. No Proxy adjustment based on bilinear matching and BDH which estimates the CL-PRE together. No, the computational cost of bilinear matching is very high and classic performance in the field.

To reduce the computational cost of bilinear matching, Seo et al. [11] introduced encryption without certificates The cloud data sharing approach avoids monopolies Twins. In this plan, the cloud creates something public and private keys for all users and sent public key for all participating users. Partial exclusion is done in the cloud. Because the truth is the main line The cloud is also used to solve partial interruptions, user interruption says to manage. However, the proposed government is doing so the cloud is both reliable and trustworthy time. From a conservative point of view, it is not recommended move the primary production system to a community where multiple tenants share around the clouds. In addition, decryption is performed twice in a system that reduces the value of unsupported in some way. Khan et al. [7] also used the El-Gamal cryptosystem and a bilinear relationship for the distribution of positive and negative information the cloud. Also, the scheme proposed in [7]. the idea of incremental cryptography that divides data into slowly block and hide obstacles.

To plan This system uses a trusted third party as a proxy to perform the task Key generation works hard, encryption, and data access control. However, total time the complexity of the bilinear equation still persists. Chen and Tzeng [8] proposed a method based on which A shared key abstraction system to secure the distribution of data between a bandage. This method uses a binary tree for calculations of keys.

However, the mathematical cost of the plan the plan is high because the rekey system is used in many places and the proposed plan. Also, the food is not good for the public cloud system because some operations require centralization mediations. Similar Rivest–Shamir–Adleman (RSA) A method based on [12] was also proposed. However, the project is a quick attack.

So, security challenges of data protection when using cloud computing must be appropriately solved and minimized. When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more doubts about the security issues when they are using this technology. So, a lot of different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are a lot of security techniques for data protection that are accepted from the cloud computing providers, and they all provide authentication, confidentiality, access control and authorization.

It was reported that 83% of the organizational workloads has shifted to the cloud platform by 2020 which raised to 90% within a year by 2021 [9]. The cloud computing industry is forecast to rise with a 14:6% compound annual rate of growth to become a $300 billion industry by 2022 as of $188 billion in 2018 [2]. Additionally, the connected IoT devices will reach 75 billion by 2025 which is 3 times the increment from 2019. IoT is the future and everything will continue to become more connected through technology that uses cloud services [2].

The following is a summary of the article's significant contributions:

The main and significant methods for data security through secure sharing in the cloud environment are reviewed in this article. We offer the information below about each strategy, including (a) how it functions for data protection and (b) the superior, outstanding, and leading solutions in the field. In order to make it simple for readers to understand the essence of the method as well as its applications, we also present potential and valuable information about each discussed solution in a tabular format, such as its working, implementation environment, success, range of the provided model, etc. A thorough and comparative study of the methodologies covered is conducted and presented in an accessible manner. Additionally, it is examined which approach works better as.

III. DATA PROTECTION IN CLOUD ENVIRONMENTS

The sharing of data securely in cloud computing is a very crucial method. The information is stored in cloud data centers. To access data from or store data into data centers through the internet, the intruders may attack our data. To avoid attackers hacking data and proper utilization of resources, we discuss many algorithms and techniques.

Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident.

Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed.

Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically.

Authentication in cloud computing ensures that the proper entity or person is getting access to the provided data from the cloud technology provider. When authentication is ensured in the cloud computing, it means that the user's identity is proved to the cloud service provider when accessing the stored information in the cloud. Public and private types of cloud are using various designs for authentication with RSA. RSA cryptosystem accepted different models for authentication like two factor authentication, knowledge-based authentication, and adaptive authentication.

IV. ACCESS CONTROL IN CLOUD COMPUTING

Access control is very important security mechanism for enabling data protection in the cloud computing. It ensures that only authorized users have access to the requested data that is stored in the cloud. There are different security techniques that enable proper access control in the cloud computing. Intrusion detection systems, firewalls as well as segregation of obligations could be implemented on different network and cloud layers. Firewall is enabling only content that is filtered to pass through the cloud network. Firewall is usually configured according defined security policies set by the users. Firewalls are usually related to Demilitarized zones (DMZ) which provide additional security of the data.

The Access Control Mechanism ACM allows controlled exposure of the confidential data to the authorized entity based on data type, user type, user's privileges, and permissions.

An Access Control Policy (*ACP*) is defined for data distribution among users. *ACP* consists of a tuple (D;U;G) where D refers to a set of data objects $D1;D2; : : : ;Dn$ to be distributed, U denotes a set of users $U1;U2; : : : ;Um$, and G is an expression or a set of expression that decide which Di can be accessed by which Uj or which Di can be allocated to which Uj or

Uj is allowed to access which *Di*. *ACP* can vary depending upon the situations and applications. ACM provides the information flow control and is suitable for any organization if access rights and data classification are properly established.

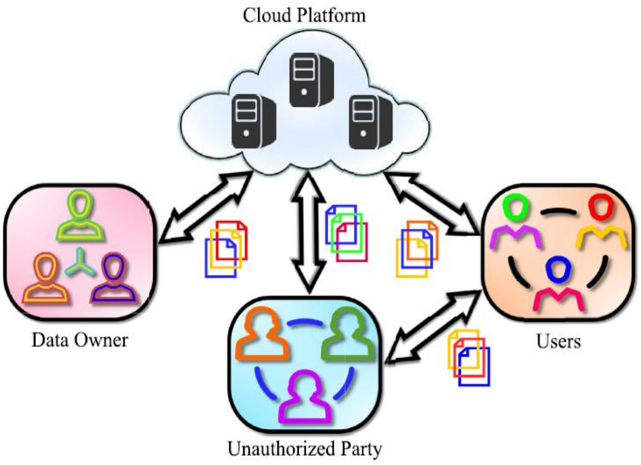

Fig 1. Cloud sharing environment

Without a proper definition of access rights, it cannot be decided whether or not the data D is being accessed by a legitimate Uj. It is important to be able to distinguish between U1;U2; : : : ;Um based on their type, privileges, and permissions for an effective ACM. There must be predefined user privileges and data secrecy levels to work properly. Access is normally granted to Uj with credentials that meet the organization's policy.

Fig. 3 represents a conventional model for access control mechanism. Three users U1;U2;U3 send the request through the internet for the six documents D1;D2; : : : ;D6. An access control policy is applied based on the users attributes, data attributes, and other essential factors; and a subset of data for which the users Uj qualify is transferred among U1;U2;U3 through the internet. Where U1;U2;U3 receives the dataset fD1;D2;D6g, fD1;D4;D5g, and fD3;D4;D5g respectively.

Nabeel and Bertino proposed a privacy-preserving policy based content sharing scheme in public clouds [54]. The approach utilized a privacy-preserving attribute-based key management scheme that protects the privacy of users while enforcing attribute-based ACPs.

The data owner performs coarse-grained encryption, whereas the cloud performs engrained encryption on top of the owner encrypted data to minimize the overhead at the data owners while assuring data confidentiality from the cloud. For the dynamic members in the cloud, a secure data sharing scheme is presented in [7]. The users can securely obtain their private keys due to the verification of their public keys. Revoked users cannot get the original data even if they conspire with the untrusted cloud to secure the scheme against collusion attacks. Previous users have no need to update their private keys when a new user joins or a user is revoked from the group to support dynamic groups.

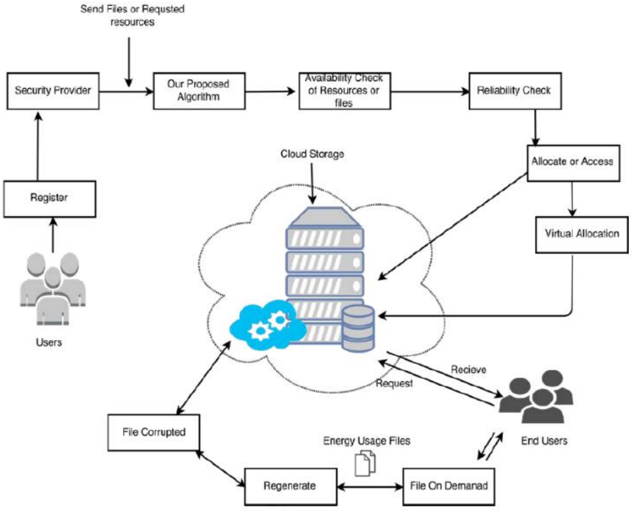

Fig 2. The Architecture of Secure Data Storing and Resource Allocation in Cloud.

V. SYSTEM MODEL

The file upload/download in a Cloud storage is shown in Figure 2. It illustrates the steps to secure, private and public data by generating the Key-Aggregate key. The data flow between users through data centers in a cloud server. The user can register and authenticate if the user exists. The authorized users can upload the file to the server. The server automatically generates a private key; the file is encrypted and stored on the servers. Any user can request to download a file initially by checking the availability of file and resources, and then the authorized user can download file by giving his private key. If the file is hacked by any intruder, another duplicate of the file stored in the distributed data center can be accessed. Here, we use a regenerative function to generate code of corrupted files. Most of the file access are based on client's demand.

The framework is used as accumulations of anything from development tools to middleware to database benefits that facilitate the creation, sending and administration of cloud applications. Tsoutsos and his colleagues [8] introduced a new based secure group sharing hidden outline for an open cloud, it successfully takes the benefit of the cloud server's assistance yet have no delicate information or data being presented to assailants and to the cloud supplier. This scheme joins strategies like a proxy signature, Improved TGDH and intermediary re-encryption composed into a procedure.

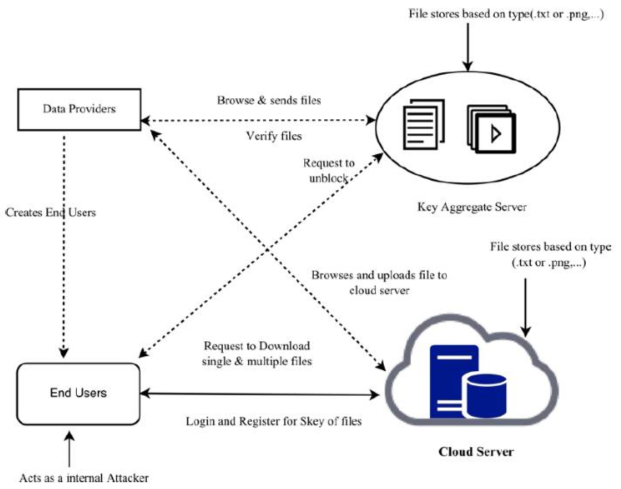
File stores based on type(.txt or .png,...)
Data Providers
Browse & sends files
Verify files
Request to unblock
Creates End Users
Key Aggregate Server
File stores based on type (.txt or .png,...)
Browses and uploads file to cloud server
Request to Download single & multiple files
End Users
Login and Register for Skey of files
Cloud Server
Acts as a internal Attacker

Fig 3. System Model: To Upload/Download a File in Cloud Storage.

Utilizing the proxy signature procedure, the group leader can progressively give the benefit of group administration to at least one picked among the people. The Improved TGDH technique helps the group to arrange and update the group key sets with the help of cloud servers, which does not require the greater part of the group individuals been online constantly. The CloudSched empowers procedures demonstrating and recreation of Cloud server farms, particularly distributing virtual machines to proper physical machines. CloudShed can deal with an expansive number of Cloud server farms, comprising of many physical machines. Diverse scheduling algorithms are utilized as a part of various data centers based on of clients' necessities [8].

The *Secure Data Sharing* methodology has the following entities.

Cloud: The cloud provides storage services to the user. The data on the cloud need to be secured against privacy breaches. The confidentiality of the data is ensured by storing encrypted data over the cloud. The cloud in the Secure Data Sharing methodology only involves basic cloud operations of file upload and download. Therefore, no changes at the protocol or implementation level on the cloud are required.

CS: The CS is a trusted party and is responsible for security operations, such as key management, encryption, decryption, the management of the ACL for providing confidentiality, and secure data forwarding among the group. The users of Secure Data Sharing are required to be registered with the CS to obtain the security services. The CS is assumed to be a secure entity in the proposed methodology. The CS can be maintained by an organization or can be owned by a third-party provider. However, the CS maintained by an organization will generate more trust in the system.

Users: The users are the clients of the storage cloud. For each data file, one user will be the owner of the file, whereas the others in the group will be the data consumers. The owner of the file decides the access rights of the other group members. The access rights are granted and revoked based on the decision of the owner. The access rights are managed by the CS in the form of an ACL file. A separate ACL is maintained for each of the data files.

The Secure Data Sharing methodology maintains a single cryptographic key for each of the data files. However, after encryption/ decryption, the whole key is not stored and possessed by any of the involved parties. The key is partitioned into two constituent parts and are possessed by different entities. The following are the keys that are used within Secure Data Sharing. Symmetric Key K: K is a random secret generated by the CS for each of the data files.

The length of K in Secure Data Sharing is 256 bits, as is recommended by most of the standards regarding key length for symmetric key algorithms (SKAs). However, the length of the key can be altered according to the requirements of the underlying SKA. K is obtained in a two-step process. In the first step, a random number R of length 256 bits is generated such that R = {0, 1}256. In the next step, R is passed through a hash function that could be any hash function with a 256-bit output. In our case, we used secure hash algorithm 256 (SHA-256).

Algorithm: Key Generation and Encryption

```
Input:
$F$, the ACL, the SKA, the 256-bit
hash function $Hf$
Compute:
$R = \{0, 1\}256$
$K = Hf(R)$
$C = \text{SKA}(F, K)$
for each user $i$ in the ACL, do
    $Ki = \{0, 1\}256$
    $Ki = K \oplus Ki$
    Add $K\_$
    $i$ for user $i$ in the ACL
    Send $K\_$
    $i$ for user $i$
end for
delete ($K$)
delete ($K\_$
$i$)
return $C$ to the owner or upload to the cloud.
```

Algorithm 2 Decryption Algorithm

```
Input:
$C$, the ACL, the SKA
Compute:
Get $K\_$
$i$ from the requesting user
Get $C$ from the requesting user or download from the cloud
Retrieve $Ki$ from the ACL
If $Ki$ does not exist in the ACL, then
    return the access denied message to the user
else
    $K = Ki \oplus K\_$
    $i$
    $F = \text{SKA}(C, K)$
    send $F$ to the user
end if
delete ($K$)
delete ($K\_$
```

The second step completely randomizes the initial user-derived random number R. The output of the hash function is termed as K and is used in symmetric key encryption [e.g., the Advanced Encryption Standard (AES)] for securing the data. CS Key Share Ki: For each of the users in the group, the CS generates Ki, such that Ki = {0, 1}256. Ki serves as the CS portion of the key and is used to compute K whenever an encryption/decryption request is received by the CS. Moreover, it is ensured by comparison that the distinct Ki is generated for every file user.

VI. CONCLUSION

We proposed the Secure Data Sharing methodology, which is a cloud storage security scheme for group data. The proposed methodology provides data confidentiality, secure data sharing without

Re-encryption, access control for malicious insiders, and forward and backward access control. The main goal of this work was to analyze and evaluate the security techniques for data protection in the cloud computing. For that purpose we analyzed and evaluated the most important security techniques for data protection that are already accepted from the cloud computing providers. We classified them in four sections according to the security mechanisms that they provide authentication, confidentiality, access control and authorization. Data protection is a challenging task in the field of cloud computing and information security. However, there is an inadequacy for the comprehensive study of the ongoing solutions. The essential and adequate information which is desired to fetch the core of the method along with the research gaps and future directions about each discussed solution is highlighted. It is investigated that no technique alone is efficient in ensuring the absolute security of the data from every directly or indirectly engaged party in the system. Moreover, with the set of highlights of addressed remarkable solutions, it is deemed that the exposed analysis will act as a milestone for the potential researchers working in the area as well as other emerging applications demanding secure data storage and sharing for its protection.

VII. REFERENCES

[1]. E. Zaghloul, K. Zhou, and J. Ren, ``P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing,'' IEEE Trans. Big Data, vol. 6, no. 4, pp. 804-815, Dec. 2020.

[2]. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ``Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331-346, Feb. 2019.

[3]. I. Gupta and A. K. Singh, ``An integrated approach for data leaker detection in cloud environment,'' J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993-1005, Sep. 2020.

[4]. Ravindra Changala, "Data Mining Techniques for Cloud Technology", in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE),Volume 4, Issue 8, Pages 2319-5940, ISSN: 2278-1021, August 2015.

[5]. R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ``A lightweight secure data sharing scheme for mobile cloud computing,'' IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344357, Apr. 2018.

[6]. I. Gupta, N. Singh, and A. K. Singh, ``Layer-based privacy and security architecture for cloud data sharing,'' J. Commun. Softw. Syst., vol. 15, no. 2, pp. 173-185, Apr. 2019.

[7]. J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, ``An efficient attribute-based encryption scheme with policy update and update in cloud computing,'' IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 650-6509, Dec. 2019.

[8]. Ravindra Changala, "Secured Activity Based Authentication System", Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[9]. Ishu Gupta, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions", VOLUME 10, 2022,IEEE Access.

[10].Mazhar Ali, “SeDaSC: Secure data sharing in clouds”,1932-8184 © 2015 IEEE.

[11].Cloud security Alliance, “Security guidelines for critical areas of focus in cloud computing v3.0,” 2011.

[12].Ravindra Changala, "Retrieval of Valid Information from Clustered and Distributed Databases", Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 21-25, September 2016.ISSN: 2455-3506.

[13].Haifeng Lu, Chuan Heng Foh, Yong gang Wen, and Jianfei Cai, “Delay-Optimized File Retrieval under LT-Based Cloud Storage”, IEEE transactions on cloud computing, vol. 5, no. 4, october-december 2017

[14].Hui Tian, Yuxiang Chen, Chin-Chen Chang,Hong Jiang, Yongfeng Huang, Yonghong Chen, and Jin Liu,” Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage”, IEEE transactions on services computing, vol. 10, no. 5, september/october 2017

[15].Y. Chen and W. Tzeng, “Efficient and provably-secure group key management scheme using key derivation,” in Proc. IEEE 11th Int. Conf. TrustCom, 2012, pp. 295–302.

[16].Ravindra Changala, “Challenges and Solutions for the Semantic Web and Future of Document Management in Enterprises ", Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 10-13, September 2016.ISSN: 2455-3506.

[17].Y. Chen, J. D. Tygar, andW. Tzeng, “Secure group key management using uni-directional proxy re-encryption schemes,” in Proc. IEEE INFOCOM, pp. 1952–1960.

Cite this article as :

Dr. Rafath Samrin, Aluri Gopi, Mangalampalli Sesha Sai Lakshmi Lavanya, K Swetha, "A Framework for Data Security and Sharing in Cloud Computing Environments by Using Cryptographic Algorithms", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 314-322, November-December 2022. Available at doi : https://doi.org/10.32628/CSEIT228641

Journal URL : https://ijsrcseit.com/CSEIT228641