RFDD – RSA Mechanism For File Distribution and Download

[1] Malathi V* , [2]Kuppaswamy Meghana , [3]Swetha S , [4]Abitha A

[1] Assistant Professor , [2,3,4] Student

[1] Panimalar Engineering College , Chennai , India

[2] Department Of Computer Science and Engineering , Panimalar Institute of Technology , Chennai , India

Abstract–Storing and sharing data through cloud has become the center of focus and demand by increasing data circulation and use within the scientific community but the integrity of the shared data remains vulnerable thus increasing the need for standard distribution method with added security scheme for preserving user confidential data. Existing schemes makes use of encryption mechanism which allows the intervention of third-party-auditing (TPA) which raises data confidentiality concerns. In this paper an RSA based encryption mechanism has been proposed which solves the above mentioned issues by eliminating the need for the third party intervention and provides an additional feature of user-authorization. The proposed system facilitates efficient file sharing to selected users and in order to access the files, request has to be sent to the sender and the user has to be granted permission thus ensuring the process of user authorization and verification. Verified users would be taken forward to key generation process where the user would be provided with a public key, and upon QR code scanning process they would be granted with the private key. Usage of RSA-Encryption mechanism provides an added advantage by solving the issue of key distribution in traditional symmetric key algorithms. Being an asymmetric algorithm, RSA eliminates the need for a key-distribution center to distribute the keys between the communicating parties. Further, the security and comparative analysis of RSA with other algorithms proves the secure nature against several security attacks and the better computational performance in context to the computational and execution time. This scheme gives access to the clients to view the shared files through the combination of both public and private keys. This proposed scheme can be implemented in any system that demands secure method for data sharing.

Index Terms–Asymmetric Keys Generation: user request, authentication , acknowledgement , QR-Scan

I INTRODUCTION

Cloud computing serves as a way of sharing information through internet for modern day business and provides a network solution for organizations having beyond handful contributors. Using cloud computing technologies, data and applications are stored at an offsite data center which can be accessed using internet. This technology significantly facilitates cloud users to upload the files and distribute to authorized users. As an emerging technology of modern day business, it manages a vast amount of confidential data, which implies it also has a business- critical responsibility to do the right thing, the right way when it comes to protecting the data. It has a responsibility towards each users to safeguard the confidential data that has been stored and interacted.

Through internet, raised share of information has been cloud-based outsourcing of data owners and sharing with verified users. For example, according to The Cisco Global Cloud Index, by 2025, the amount of data stored in the cloud would be around 1.5 zettabytes. Increasing use and demands leads to the rise of increasing security concerns of the confidential data. These information are a primary focus for cyber criminals and includes any information that can identify an individual.

A data incident can damage and disrupt the business operations and can create a negative impact on the growth, lead to regulatory penalties and fines ,transforms users as an easy target for the hackers and result in the loss of client trust relationships. Thus it adds up to the responsibility of the File Distributers to ensure and facilitate a secure mechanism for file sharing and distribution over internet. The existing schemes that has been proposed to reduce user burden has a disadvantage of involvement of Third party auditing(TPA). As a method of overcoming the mentioned disadvantage, new RSA-based encryption system has been presented as an answer to the aforementioned issues, guaranteeing secure data sharing across the cloud and limiting access to only verified users. The contribution can be summarized as follows.

- A model has been established to ensure secure data sharing through cloud servers and authorized access has been enabled. This provides an advantage of elimination of TPA in computing mechanisms thus ensuring data security. User identification attributes have been taken into consideration.
- The scheme implements RSA encryption method as an encryption mechanism to promote the data security. This method involves the process of public and private key generation mechanism thus enabling user authorization process. Only the authorized users would be provided with the private keys thus restricting the visibility of the file to verified users. Further, Key generation mechanism provides the advantage of faster encryption process.
- As an added feature, the proposed scheme makes use of QR scanning process to enable the users to scan the bar code for private key generation which eliminates the chance of reading the sensitive data contents by the unauthorized parties.

.

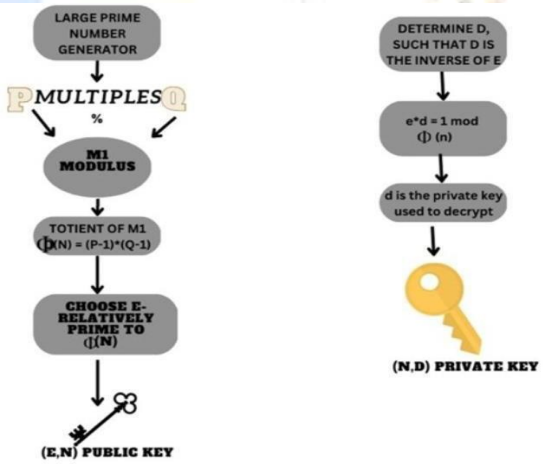

Fig 1. Key generation in RSA

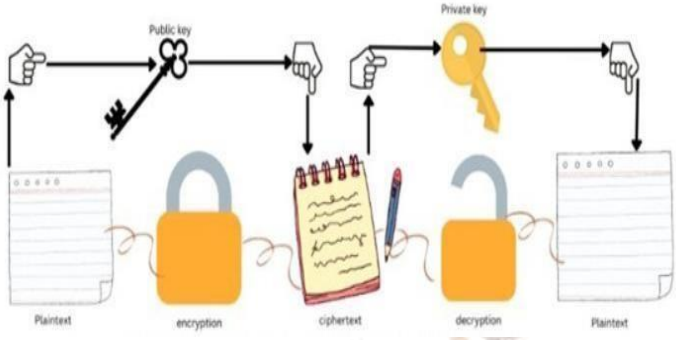

Fig 2. RSA encryption and decryption

Thorough security analysis shows that the proposed system simultaneously accomplishes data secrecy, protection against security attacks, tag consistency, and access control. It is difficult to computationally factor large integers into prime numbers, and the effectiveness is demonstrated by the fact that it uses one of the two keys to encrypt and the other to decrypt, ensuring the confidentiality, integrity, authenticity, and non-reputability of data and electronic communications.

II RELATED WORK

The Provable Data Possession (PDP) paradigm[1],was first put forth by Ateniese et al., who used homomorphic verifiable tags and a challenge- response mechanism to check the integrity of the data. Jules et al. suggested the Proofs of Retrievability (POR) concept to support data retrievability. Several expanded PDP or POR-based solutions have been put up to address various issues in public auditing.[2]-[5]Yang X lu. introduced the Oruta public auditing technique for shared data in cloud that protects user privacy while taking into account the applications of cloud data shared by group users. They used a homomorphic authenticable ring signature-based system, which enables a public auditor to check the shared data without having to download it all fromthe cloud.[3]-[7] .Large groups in the cloud cannot use it since the auditing overhead linearly rises with the number of group users..

[8]-[9]Wang et al. developed a public auditing system in 2012 that relies on group signatures to preserve the identity privacy of cloud users. This system facilitates dynamic joining and exiting in addition to safeguarding the group members' privacy regarding their identities. With larger groups, their plan becomes less effective, and it is impossible to identify the bad group members. Li et al. presented a tiny integer-based privacy-preserving technique. The fact that the audited data are randomly chosen and compressed gives this technique the advantage of being resistant to quantum assaults as well as being resistant to the inquisitive auditors attack on the auditing content. [10] Jianting Ning has proposed a dual access control mechanism that uses Intel SGX to enable user-level code to allocate private memory areas known as enclaves that are intended to be shielded from Processors operating at higher privilege levels.

A decentralized application is used to manage the login information. The proposed architecture is determined to be practical, safe, and capable of measuring up to the performance of the well-known blockchain benchmark platform. A patient-controlled, safe, and privacy-preserving EHRs system based on consortium blockchain was proposed by Shunrong Jiang. This makes EHR exchange more effective and increases control over the healthcare industry. The aforementioned needs are completely met by the characteristics of blockchain, such as decentralization , immutability, and auditability. Moreover, this approach groups transactions into different kinds to ensure effective block elimination.

III PROBLEM STATEMENT

The system model, threat model and design objectives are being described in this section.

The system model, threat model and design objectives are being described in this section.

A. System model:

Three entities make up the proposed system model, and each of their description is given below:

- Centralized Key production center (CKP): The CKP is in charge of first configuring the entire system. In proposed model, database acts as the key generation and storage center of both the public , private , as well as the request and response messages issued by the user and the providers respectively.

- File distributors (FD) : The FD allows access for the users. proposed scheme of FD include Team Leader and management. The team Leader upload the files to the cloud server in an encrypted format. Verifying the requests of the user, the team leader shares their response to the management. The response would be positive for approved users and negative for unauthorize users. Upon verification of the team leader's response, the management proceeds with the process of key generation and stores it in the database.

- Users : The users consists of staff members who can be categorized as authorized and unauthorized . Upon viewing the shared file, the users can raise a request to the team leaders for downloading the file which would be stored in the Database and forwarded to the users. After the process of successful verification, the user would be provided with public as well as private keys using the combination of which The user can scan the QR- code and download the file in an decrypted format.

B. Issues:

- **Safety issue:** Two different types of integrity threats exist in relation to shared data integrity. One is that outside attackers could tamper with the shared data in the cloud, preventing group users from accessing the right information. The shared data in the cloud could also be corrupted or lost as a result of human or program error.

- **Data expose issue:** A TPA may receive certain privacy information from the verification metadata during the auditing process as a trusted third party and curious verifier.

C. Construction purpose:

Based on the threat models, The objectives for the proposed systems have been set as follows:

- Data security: It is not feasible for any opponent, including the CSP or unauthorized users, to obtain any meaningful information.
- defense against a brute-force attack.
- Usage restriction : The suggested strategy should make sure that all authorized users chosen by the data owner, as well as the data owner, can access outsourced encrypted data.
- Resistance to timing attacks.

IV PRILIMINARIES

This section outlines groupings of bilinear, Bilinear maps, splitting , Pollard's , Elliptic curve method

A. BILINEAR MAPS:

Let P and P r be two multiplication cyclic clusters. It is considered to abide to the following functionalities:

- Bilinguality : For X,Y ∈ Z and U,V∈ Z, e(P pow(i) , Q pow(j),(p pow(u) and Q pow(v)) equals e(u ,v) pow (i, j).
- Not-unity : not equating the value of one..
- Processability : Existence of rules to compute generators of p.

B.ELLIPTIC CURVE METHOD

For the purposes of the current ECC, an elliptic curve is a plane curve over a finite field made up of points obeying the equation y2=x3 + axe + b. Each point on the curve in this illustration of elliptic curve cryptography can be mirrored over the x-axis without changing the shape of the curve. Any non-vertical line will only come into contact with the curve three times or less.

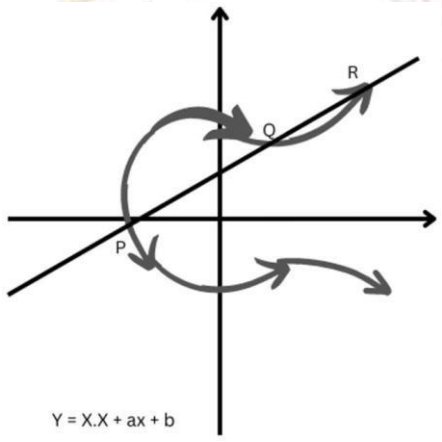

Fig 3 Elliptic curve cryptography

C.SPLITTING METHOD

Splitting is tedious task compared to a thorough search for the RSA private Key. One need only search for all primes up to the square root of n since a composite number N must have a prime number divisor = n pow (1/2) in order to be divisible by prime numbers.

D.POLLARD'S P-1 METHOD

This is a special purpose factoring method , which relies on a special property of a divisor of n. Two prime factors can be applied for n only when n is a power of a.

V PROPOSED SCHEME

A.SYSTEM ARCHITECTURE

The system architecture of RSA based cloud sharing has four entities..

- Database : The first and the foremost entity which serves as the centralized server for storing the requests and retrieving the information from the storage.
- Management : The second important entity in the working model. The important function played by this entity is addition of the team leader to the working system. Main functions of management include staff acknowledgement and key generation.
- Team Leader : Team Leader's role starts when he/she uploads the file as safe locked file. Main functions of team leader include staff verification and forwarding process.
- Staff : This entity is considered to be the initiating entity which starts the work flow. The working starts when the staff send request to the team Leader.

B.SYSTEM INITIALIZATION

The system initialization in the proposed scheme consists of three parts.

- FD's shares files by setting his/her own authorization policies and by encrypting the selected data using asymmetric protocol standards.
- Users send requests which are stored in the CKP's and later reviewed by the FD's for verification process.
- Upon successful verification , CKP gives the staff members , the access to the files as follows:

Algorithm 1: RSA Encryption Algorithm |

1 **Variables:**
  Public Key: Tuple (e, n)
  Private Key: Integer d
  Plaintext: P
  Ciphertext: C
2 **Functions:**
  Carmichael's Totient function: $\phi(n)$
3 **Key Generation:**
  Choose two large primes p and q such that $p \neq q$
  Calculate $n = p \times q$
  Calculate $\phi(n) = (p-1) \times (q-1)$,
  Choose e such that $gcd(e, \phi(n)) = 1$
  Calculate $d = e^{-1} mod(\phi(n)))$
4 **Encryption:** $C = P^e \ mod(n)$
5 **Decryption:** $P = C^d \ mod(n)$

Fig 4 RSA Encryption

C.INTERACTION OF THE ENTITIES

Registered team leaders shares their files in an encrypted format to the database. The team leader would be provided with a share file option. Once the data is been shared, the staff members would be notified in their view file column .Staff's would send a request message to the tam leader. The request would be approved and forwarded to management if the user is verified. Authorized users would be moved forward to key generation process and provided with a QR code. Upon successful scanning process the file would be downloaded by the staff members.

Fig 5. Download page

D.DESIGN OBJECTIVES

Data confidentiality: Any adversary including the CSP of unauthorized users cannot feasibly extract any useful information, Resistance to brute-force attack, Access control, Tag consistency, Efficiency, Resistance to timing attacks.

VI PERFORMANCE EVALUATION

- **TIME COMPLEXITY ANALYSIS**

It has been identified that there is no precise time complexity of RSA, as various implementations have significantly different complexities and the time varies typically much less than from an implementation to the other. Asymptotic time complexity for an implementation of RSA using elementary algorithm , commonly used in practice is *O(n) pow 3* for private key use. where the public modulus N has n bits and public exponent e has a fixed size.

E = 2 pow (2) pow(4) + 1 = 65537(F4) as customary.

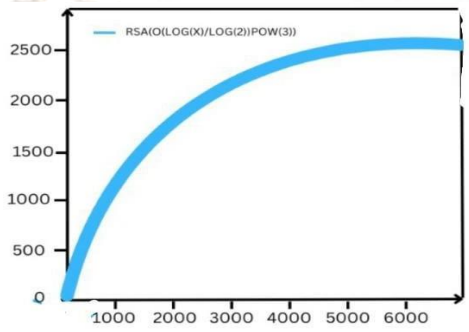

Fig 6. Time complexity analysis

- **POWER ANALYSIS**

A new form of attack was introduced on smart cards and cryptographic tokens called power analysis. These attacks are mounted by monitoring the token's power consumption varies significantly during different steps of the cryptographic operation, an attacker can recover the secret information.

- **COMPARATIVE ANALYSIS**

The comparison of RSA algorithm over DSA over the Execution time taken and ECC on the basis of encryption decryption time has been made . The results of the comparative analysis has been tabulated as follows.

INPUT FILE SIZE	RSA	DSA
30	5.637362	18.17544
45	11.27472	27.26315
60	16.91209	36.35087
75	28.18681	45.43859

TABLE 1. COMPARISON OF RSA AND DES

	Encrypt	Decrypt	Total
RSA	0.8	0.3	1.1
ECC	1.05	1.86	2.91

TABLE 2. COMPARISON OF RSA AND ECC

- **EXPERIMENTAL IMPLEMENTATION OF RSA**

RSA algorithm has been implemented using HTML,JAVASCRIPT as an experimental and results has been recorded.

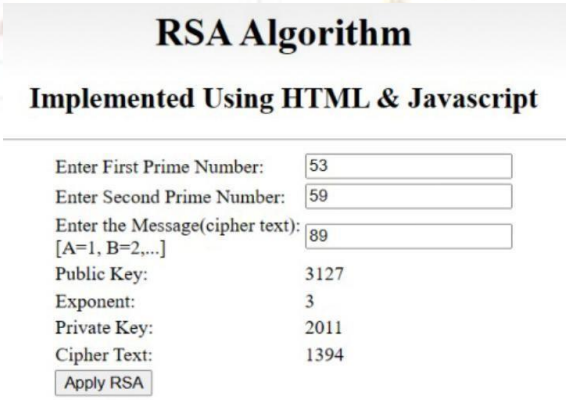

Fig 7. RSA Implementation

VII SECURITY ANALYSIS

The safety properties are analysed by listing out the possible attacks and counter measures to resist the respective attacks in order to achieve data confidentiality and integrity. The possible attacks can be listed as follows:

A. SELECTED DECRYPTED MESSAGE ATTACKS:

Using the extended Euclidean algorithm, the attacker might determine the plain text from the encrypted text in this kind of attack.

Counter measure : This threat can be prevented by inserting encrypted pieces of data and reviewing the decrypted versions of data that has been inserted.

B. DECOMPOSITION ATTACK

The values of the secret key can be discovered if the attacker can determine P and Q using N.

Counter measure: This can be prevented by setting the value of n greater than 300.

C. ALL POSSIBLE MEANS ATTACK

This requires testing with every potential secret key.

Size of N	Time to break RSA in milliseconds
7	0.002
8	0.002
9	0.561
10	4.206
11	12.110
12	38.561

Fig 8.Attacking standards using brute force

Counter measure : Locking the accounts.

D. SECRET POWERING THREAT

The RSA decryption and signing are very compute -intensive operations, which take time linear to the length of the private exponent d. Thus some low-power devices may want to use a small d instead of a random one, in order to improve performance. However an attack due to M.Wiener shows that the choice of a small d can lead to a total break of the system. More specifically, he showed that if n is the modulus and d is the private exponent , with d<1/3(n)pow(1/2), then given the public key(e ,n), an attacker can efficiently recover d.

The safety ratings are determined on the basis of the attacks and counter measures implemented to resist the attacks. The general counter measures implemented by RSA revolves around the key size and reducing the message bit size. Security nature can be increased by carefully selecting the size of the key, Parameter properties , and cipher text formulation for experimental details. The preferred exponent value is 65,537 for more secure computation. The plain text messages must always be ensured to be in an encrypted format.

VIII RESULTS

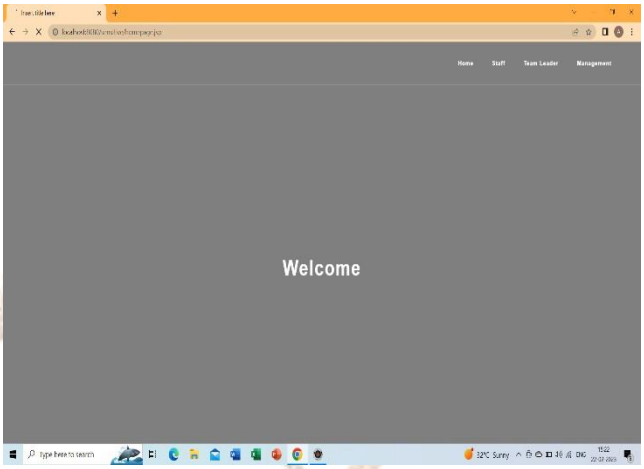

Fig 9. Home page

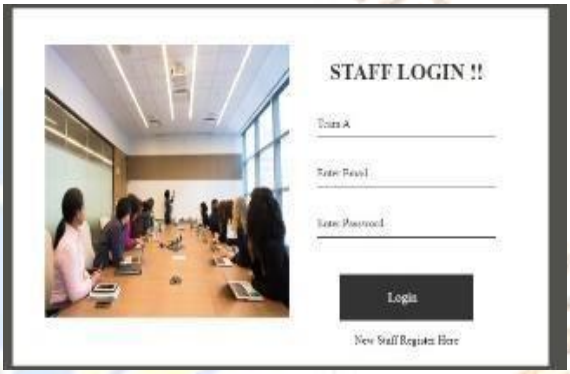

Fig 10. staff login page

Fig 11. Staff request page

Fig 12. Team leader response page

After receiving the response from the team Leader, the staff's would be able to download the file in the decrypted format from the database.

IX CONCLUSION

The proposed system forms a solution architecture that address the major threats and issues faced by cloud computing which includes un-authorized access and insecure interfaces by providing a scheme that facilitates secure and efficient data sharing. It also promotes selective disclosure of file contents and user-authorization. The security of the system is built by RSA encryption mechanism that facilitates secure data transfer over internet compared to traditional methods along with the usage of key-generation (public and private) and exchange mechanisms that provides toughness in breaking the keys and resistance against cybersecurity attacks such as plain-texts, short messages, chosen cipher and cycling attacks and provides an advantage of faster computation speed when compared to the traditional methods. The need for third-party auditing system (TPA) is eliminated in this scheme. An additional attribute of QR-code scanning has been added that cannot be hacked. As a part of future work, the disadvantage of present system such as computational complexity due to key size can be mitigated by enhancing the security scheme to hybrid encryption. At second level, circuit-level intrusion detection system can be implemented along with the application level gateway firewalls to detect and prevent malicious intruders thus presenting an enhanced system for secure data sharing over internet with a real world anonymous database system.

X REFERENCE

[1] Mukta, R., Martens, J., Paik, H.Y., Lu, Q. and Kanhere, S.S., 2020, December. Blockchain-based verifiable credential sharing with selective disclosure. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 959-966). IEEE.

[2] Yang, X., Lu, R., Shao, J., Tang, X. and Ghorbani, A.A., 2020. Achieving efficient secure deduplication with user-defined access control in cloud. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), pp.591-606.

[3] .Sundari, S. and Ananthi, M., 2015, February. Secure multi-party computation in differential private data with Data Integrity Protection. In *2015 International Conference on Computing and Communications Technologies (ICCCT)* (pp. 180-184). IEEE.

[4] Kakade, N. and Patel, U., 2020, July. Secure Secret Sharing Using Homomorphic Encryption. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE..

[5] Kamal, A.A.A.M. and Iwamura, K., 2021. (Server-Aided) Two-Party Multiplication of Encrypted Shares Using (k, n) Threshold Secret Sharing With N≥ k Servers. *IEEE Access*, *9*, pp.113117-113129.

[6] Liu, D. and Lee, J.H., 2020. CNN based malicious website detection by invalidating multiple web spams. *IEEE access*, *8*, pp.97258-97266.

[7] Jiang, S., Wu, H. and Wang, L., 2019, December. Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium blockchain. In *2019 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

[8] Fu, A., Yu, S., Zhang, Y., Wang, H. and Huang, C., 2017. NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users. *IEEE Transactions on Big Data*, *8*(1), pp.14-24..

[9] Wang, Z., Huang, D., Zhu, Y., Li, B. and Chung, C.J., 2015. Efficient attribute-based comparable data access control. *IEEE Transactions on computers*, *64*(12), pp.3430-3443..

[10] Ning, J., Huang, X., Susilo, W., Liang, K., Liu, X. and Zhang, Y., 2020. Dual access control for cloud-based data storage and sharing. *IEEE Transactions on Dependable and Secure Computing*, *19*(2), pp.1036-1048..

[11] Hou, H., Ning, J., Zhao, Y. and Deng, R.H., 2021. A traitor-resistant and dynamic anonymous communication service for cloud-based vanets. *IEEE Transactions on Services Computing*, *15*(5), pp.2551-2564.

[12] Panchal, G., Samanta, D., Das, A.K., Kumar, N. and Choo, K.K.R., 2020.Designing Secure and Efficient Biometric-Based Access Mechanism for Cloud Services. *IEEE Transactions on Cloud Computing*, *10*(2), pp.749-761.

[13] Ali, M., Sadeghi, M.R. and Liu, X., 2020. Lightweight revocable hierarchical attribute-based encryption for internet of things. *IEEE Access*, *8*, pp.23951-23964.

[14] Jin, W., Xu, R., You, T., Hong, Y.G. and Kim, D., 2020. Secure edge computing management based on independent microservices providers for gateway-centric IoT networks. *IEEE access*, *8*, pp.187975-187990.

[15] Rasori, M., Perazzo, P., Dini, G. and Yu, S., 2021. Indirect revocable kp-abe with revocation undoing resistance. *IEEE Transactions on Services Computing*, *15*(5), pp.2854-2868.

[16] Susilo, W., Jiang, P., Lai, J., Guo, F., Yang, G. and Deng, R.H., 2021. Sanitizable access control system for secure cloud storage against malicious data publishers. *IEEE Transactions on Dependable and Secure Computing*, *19*(3), pp.2138-2148.

[17] Huang, K., Zhang, X., Mu, Y., Rezaeibagha, F. and Du, X., 2021. Bidirectional and malleable proof-of-ownership for large file in cloud storage. *IEEE Transactions on Cloud Computing*, *10*(4), pp.2351-2365.

[18] Xiong, L., Han, X., Yang, C.N. and Shi, Y.Q., 2021. Robust reversible watermarking in encrypted image with secure multi-party based on lightweight cryptography. *IEEE Transactions on Circuits and Systems for Video Technology*, *32*(1), pp.75-91.

[19] Zhang, Y., Xu, C., Cheng, N. and Shen, X., 2021. Secure password-protected encryption key for deduplicated cloud storage systems. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), pp.2789-2806..

[20] Han, D., Pan, N. and Li, K.C., 2020. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), pp.316-327.

[21] Xu, S., Ning, J., Huang, X., Li, Y. and Xu, G., 2021. Untouchable once revoking: a practical and secure dynamic EHR sharing system via cloud. *IEEE Transactions on Dependable and Secure Computing*, *19*(6), pp.3759-3773.

[22] Huang, Q., Chen, L. and Wang, C., 2022. A parallel secure flow control framework for private data sharing in mobile edge cloud. *IEEE Transactions on Parallel and Distributed Systems*, *33*(12), pp.4638-4653.

[23] Yang, K., Shu, J. and Xie, R., 2022. Efficient and Provably Secure Data Selective Sharing and Acquisition in Cloud-Based Systems. *IEEE Transactions on Information Forensics and Security*, *18*, pp.71-84.

[24] Zhao, C., Xu, L., Li, J., Fang, H. and Zhang, Y., 2022. Toward Secure and Privacy-Preserving Cloud Data Sharing: Online/Offline Multiauthority CP-ABE With Hidden Policy. *IEEE Systems Journal*, *16*(3), pp.4804-4815.

[25] ABI-CHAR, P.E., 2022, July. A BP-based Key Management Protocol for Data Sharing on Cloud Storage with Access Control. In *2022 45th International Conference on Telecommunications and Signal Processing (TSP)* (pp. 132-138). IEEE.

[26] Upadhyay, D. and Sampalli, S., 2020. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, p.101666.

[27] Agyekum, K.O.B.O., Xia, Q., Sifah, E.B., Cobblah, C.N.A., Xia, H. and Gao, J., 2021. A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. *IEEE Systems Journal*, *16*(1), pp.1685-1696.

[28] Guo, W., Qin, S., Gao, F., Zhang, H., Li, W., Jin, Z. and Wen, Q., 2020. Dynamic proof of data possession and replication with tree sharing and batch verification in the cloud. *IEEE Transactions on Services Computing*, *15*(4), pp.1813-1824.

[29] Wang, J., Zhang, R., Li, J., Xiao, Y. and Ma, H., 2021. SeUpdate: Secure Encrypted Data Update for Multi-User Environments. *IEEE Transactions on Dependable and Secure Computing*, *19*(6), pp.3592-3606.

[30] Ge, X., Yu, J., Hao, R. and Lv, H., 2021. Verifiable Keyword search supporting sensitive information hiding for the cloud-based healthcare sharing system. *IEEE Transactions on Industrial Informatics*, *18*(8), pp.5573-5583.