Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

Multi User Keyword Search on Multi Owner's Encrypted Data

* A.V.M.B. Aruna[1]
Department of Computer Science and Engineering
Periyar Maniammai Institute of Science & Technology, Vallam, Thanjavur 613403, Tamilnadu, India.

* M. R. Santhoosh[2]
Department of Computer Science and Engineering
Periyar Maniammai Institute of Science & Technology, Vallam, Thanjavur 613403, Tamilnadu, India.

A. Sharuk Mohamed[4]
Department of Computer Science and Engineering
Periyar Maniammai Institute of Science & Technology, Vallam, Thanjavur 613403, Tamilnadu, India.

G. Ranjith[5]
Department of Computer Science and Engineering
Periyar Maniammai Institute of Science & Technology, Vallam, Thanjavur 613403, Tamilnadu, India.

* A. Raja Rajeswaran[3]
Department of Computer Science and Engineering
Periyar Maniammai Institute of Science & Technology, Vallam, Thanjavur 613403, Tamilnadu, India.

Abstract - The data owner cannot rely on the remote server situated in a building to provide access to the data since cloud services remove that data from cloud service customer (individuals or businesses), denying them full control over these data. As a result, it is now challenging to provide secure network access in public cloud services. Here, we suggest an effective access control approach that combines time and attribute variables for moment data in public clouds. The suggested framework can implement a perfectly alright and timed release access control system: After a certain period of time, only one user with a fulfilled set of attributes can access the data. Each file's access policy is established by the data holder (Owner) based on a particular set of attributes one and or more release time points. The file is then encrypted according to the chosen policy before being uploaded. We present an effective method to provide safe fine-grained network access for time-sensitive data in public cloud storage by combining Time based access control and the Advanced Encryption Standard algorithm. The data holder can independently specify end user and the appropriate access permission release times under the proposed method. In addition to accomplishing the purpose, it is demonstrated that owners, users, as well as the trusted server are under no significant load. We integrate two cutting-edge cryptographic methods, namely ECC and time-based access mechanisms, to create a scalable as well as perfectly alright access control for outsourced time-sensitive data.

Keywords—Cloud computing, Security, Access control, Time Sensitive, Cryptography.

I. INTRODUCTION

"Cloud computing" is a style of Internet-based computing that quickly makes data and resources from a network of computers and devices available to other hardware and computers. It is a framework for granting everyone access, whenever they need it, to a variety of reconfigurable computational power (such as servers, networking, memory, apps, and services), that can be quickly installed and withdrawn with little administrative work. Due to storage as well as cloud computing alternatives, users and companies can store and process data in either privately held or third-party datacenters that may be distant from of the user, ranging in distance from inside the city across the world. Similarly to utilities (like the power grid) over an electrical network, public cloud relies on resource sharing to achieve consistency and scale economies. Advocates assert that businesses can minimize upfront infrastructure expenditures by using cloud computing (e.g., purchasing servers). Additionally, it helps firms to concentrate on their core operations rather than investing time and resources on computer infrastructure.

Additionally, proponents assert that cloud computing allows information technology (IT) staff to more quickly modify funds to attain fluctuating as well as unpredictable business needs and helps businesses get their apps up and operating more quickly, more manageably, and with less maintenance. Most cloud service providers follow the "pay as you go" principle. In the event that administrators do not adjust to the internet pricing model, this will result in unexpectedly high costs. To protect data, applications, and the clouds computer networks as a whole, a wide range of policies, techniques, and controls are applied. This is known as cloud computing, or just cloud security in computer terms. It relates to computer security, data security, and data security. Due to cloud computation and storage, users have the choice to store and analyse sensitive data in outside data centres. Businesses merely employ the cloud inside a range of distinct service models and deployment paradigms (using abbreviations such SaaS, PaaS, and IaaS) (public, private, hybrid, and community).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181, Vol. 12 Issue 08, August-2023

Private cloud: An exclusive company's usage of a cloud infrastructure is known as a private cloud. It might be managed by a company or another person. Using an underlying pool of real resources, a private cloud offers computing power as a service within a virtual environment. Resources in a private cloud are only accessible by consumers of any firm, enhancing the security and privacy policy of that company. Because it was initially managed by one company, private cloud usage is more secure than using other clouds [18]. A cloud computing deployment methodology is depicted in a block diagram in Figure 1. Public cloud: In the public cloud, the CSP offers the necessary resources, including servers, networks, data centres, etc. [19]. Users of the public cloud can make payments based on how much use they have incurred. It enables IT firms to modify their cloud use in accordance with their needs [20]. The public cloud is a shared network or cloud that is used by users or customers from several different enterprises. There can be a lot of attackers due to the big number of users from various organisations. Security concerns are therefore significant in the public cloud. There is less security in the public cloud than in other clouds. If the CSP checks the cloud server often, this issue can be reduced. Community cloud: In a community cloud, a community of several companies shares infrastructure or a cloud environment [21]. A unifying objective must exist for all of these groups. Each of these businesses or a third party is in charge of managing the community cloud. National security purposes are occasionally served by using the community cloud. Community clouds include "Open Cirrus." Several scientists or academic institutions utilise "Open Cirrus" as their testbed. For inter-agency and cooperation requirements, the community cloud is also employed. Cloud hybridization: Cloud hybridization combines public and private clouds. The administrator in charge of it oversees it [22]. Using public, private, and community clouds to deliver IT solutions also allows for safe access control between users and cloud service providers. If users, CSPs, and DOs make a lot of requests for data access in the hybrid cloud, other clouds are not affected by those requests.

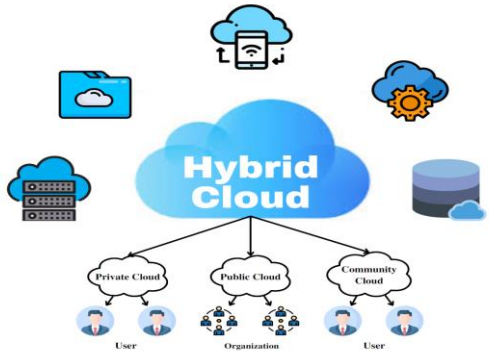

Fig. 1 Cloud Architecture

Cloud providers (businesses that deliver software, platforms, or infrastructure as a service via the cloud) and their clients are both affected by the security risks associated with cloud computing (i.e., companies that host applications & store data on the cloud). It's crucial to remember that these two parties each share responsibility for security. While users must take steps to make their apps stronger and employ secure login credentials and processes, service providers must maintain the security of their infrastructure and safeguard users' data and applications.

II. LITERATURE REVIEW

A method for accessing and managing attachable data storage devices was created by Yongdong Wu et al. [1]. With the help of this method, data owners may provide access based on user qualities rather than specific conditions. Using a policy-based attribute encryption technique, it also guarantees confidentiality and restricted media access. The system employs MCPC-ABE and multi-message cryptography to encrypt many messages in a single ciphertext. It is appropriate for mobile devices with limited resources since the workload of computationally expensive activities is transferred to cloud servers without jeopardising the security of personal data. With a cloud platform accessible, the system is safe from individual collision attacks and functions well on mobile devices, however decryption could be delayed for short-stop devices. The goal of future research is to hasten the decoding procedure for such devices. The optimal access control technique must be used in order to distribute media-friendly content in a regulated manner. Attribute-based encryption (ABE) technique was created for fine-grained data access control by Jun Hur et al. [2]. An encryptor can predetermine the attributes needed for decryption using CP-ABE. As a result, there is no longer a requirement for traditional access control or reliance on digital storage servers. The key generation centre (KGC) in CP-ABE, however, has a significant escrow problem because it can decrypt any encrypted content and creates a privacy hazard. Maintaining security necessitates key cancellation or replacement, particularly in ABE where a limited number of users may share characteristics. All of an organization's customers may be impacted by this. In spite of this, CP-ABE continues to be helpful in minimising the necessity for exchanging and maintaining public key credentials.

Allison Lewko, et.al… [3] The MA-ABE system was used to suggest a novel with the exception of assessing the initial set of community location limits, this approach does not need global synchronisation. The system creates public keys and distributes non-public keys to distinct operators to enable the auctioning of events. Using the Chase concept of universal IDs, the system also integrates personal sources provided to the same client through certain government processes. The device is more widely available and safer because it doesn't need a specific expert or depend on the government. To make the system resistant to conspiracies, there are still obstacles to be addressed. To self-preserve the core cohort and deal with collisions is the primary objective.To sum up, Allison Lewko and associates developed a novel method that does away with global

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181, Vol. 12 Issue 08, August-2023

synchronisation by utilising the MA-ABE system. The system links individual sources using universal IDs and supports event auctioning. The device is more widely available and safer because it does not require a critical specialist or government dependency. To make the system resistant to conspiracies, there are still obstacles to be addressed. To self-preserve the core cohort and deal with collisions is the primary objective. Jianwei Chen, et.al, [4] the creation and application of cloud computing. The concept's central element, cloud storage, enables the storage of data across various places. Before it may be utilised widely, three issues need to be fixed. Security of documents and preventing unwanted access come first. In order to prevent high-quality users from accessing shared resources, access controls must secondly be more complicated. Lastly, it must be feasible for clients to revoke their benefits from shared aid. These problems can be addressed with ABE, especially CP-ABE. This protocol eliminates the need to rely on the cloud to block unauthorised access by allowing a predetermined set of attributes to be specified for decrypting encrypted text.Currently, ABE protocols only let one authority to manage the mystery keys for each user. In conclusion, Jianwei Chen and associates examined the growth of cloud computing. Although cloud storage is an essential component, three issues with data security, access controls, and client revocation need to be fixed before it can be extensively employed. ABE, in particular CP-ABE, is an appropriate approach for dealing with these problems. It removes the need to rely on the cloud to block unauthorised access and permits a defined set of attributes for decrypting encrypted text. The mystery keys for each user may presently only be handled by one authority per ABE protocol.

Ling Cheung, et.al, [5] provided CP-ABE technology Under the Based algorithm Bilinear Diffie-Hellman (DBDH) assumption, It is simple to settle on basic text material for this. The gates that make up the entrance controls in this setup can work on both fantastic and terrifying qualities. Next, using one-time signatures, a delegated cypher text guarded permission is created using the Canetti-Halevy-Katz method. The Components assumptions and the enforceability of a monogram primitive are reduced by the security proof. Because robust existentially enforceable signatures may be generated under the traditional computational Diffie-Hellman (CDH) postulation, the security of the CCA method reduces to DBDH as well as CDH. According to the most accurate information, that is the most significant official CCA protection evidence for CP-ABE. Present an alternative that has significantly faster encoded operations and smaller cipher texts. The key idea is to organise the characteristics into a hierarchy so that just a small number of organizational components are required to make up all of the characteristics inside the machine. This green version has been proven to be CPA friendly. We may also make improvements to our CCA ease programme in a similar way. We recommend the use of distinct CP-ABE encryption timings for discontinuous ordinary form tips. As we seek adaptive ID fortifying proofs for CP-ABE, it safety of such a belief remains a challenge. Limitations: As businesses move their IT infrastructure to the cloud, they face a number of difficulties. While adopting cloud computing might be less expensive than keeping up an independent IT infrastructure, SMEs might not have to deal with all of these difficulties. The adoption of cloud computing by SMEs may be properly assessed with the use of a flawless cost-benefit trade-off [5]. We examine every conceivable issue that might prevent certain SMEs and large businesses from adopting cloud computing in this part.

However, because the randomized messenger variant was so contentious, it became a significant ongoing challenge to create unique encryption techniques that would comfortably fit inside the current paradigm. To start working toward accomplishing this objective, Canetti et al. [8] create a persona-based encryption conspiracy that, despite having a worse overall security presentation, is easily secure with uncontrolled advent. In this flawed idea, also known as a unique person security, an antagonist tries to learn more about the target of their long-term ill will. Inside the traditional person-based edition, the adversary is free to choose someone anyway they see fit. The safety of the strategy depends on the integrity of a Components issue, and the development is actually quite ineffective. In exchange, Boneh and Boyen [9] created efficient character-based encryption techniques which do not depend on the random prophetic technique and both are independently secure in the particular character set. The top framework, whose safety is based on the Component hassle, is comparable to a skillful modern character wholly encrypts frameworks (see following area). Although the second approach is far more effective, its safety concepts can be used to address a unique DBDHI issue. A subsequent enhancement by Boneh and Boyen [10] is Security declines to a DBDH problem and is proven to be entirely uncontrolled by strange prophets. The suggestion, however, is improbable and is merely used as an example in a hypothetical context to demonstrate there are sentient encryption techniques that are entirely secure without any need for special prophecies. In the end, Waters [11] improves this without strange prophesies, it produces a different method that is successful and completely comfortable. Its defence against the DBDH problem also is becoming less reliable.

Hierarchical person-based encryption was proposed by Hurwitz and Lynn [12], allowing lower-level experts to obtain recommendations from higher-level experts. To make the procedure simpler, this idea may be used with character-based encryption. This approach uses a cryptographically signed individual key generator. A root secret key producer and a placement secret key producer can be used to provide multilevel dependent cryptography. This enables clients to be connected to both their own distinct identity and their identity within their particular place. A nearby manufacturer of private keys, who gets its private key from the source producer of private keys, is where customers may get their secret key. With inclusive domains and micro subdomains,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

this command chain may be advanced to new heights. Multiple-level person-based encryption has been proposed by Gentry and Silverberg. [13]. The BDH problem was addressed by Boneh and Boyen, who created a technique for creating a multi-level symmetric cryptography with random prediction. Nevertheless, this technique performs best in less reliable precise ID displays. This strategy, which makes use of arbitrary prophets, is an extension of Bone Franklin's strategy [14]. Complex command chains reduce the effectiveness of the aforementioned strategies. A multi-level human-based encryption method that maintains a consistent decryption time along the command chain has been suggested by Boneh, Boyen, and Goh. [17] Even in the presence of a BDHE challenge and unusual signals, it is accurate.

A completely encrypted system utilising fuzzy identification has been presented by Sahai and Waters in [15]. Characters in this cryptography are seen as fuzzy entities rather than a collection of symbols or tidy functions. Theoretically, communications encoded with public and private keys can be deciphered if d (d, d') and failure-tolerant versions are employed. Biometric identity has several uses for fuzzy identification-based encryption. Nevertheless, when employing biometric IDs as keys, the Sahai-Waters scheme's security deteriorates owing to the changed DBDH difficulty, necessitating the need for error resilience.While it was developed earlier, Cocks' identity-based encryption system is comparable to Boneh-[19]. Franklin's The plan is based on a problem known as the modulo quadratic residue issue, where N = p, q, and p, q are top values of Z. Although offering enormous determinant writings, the technique is not as efficient as other mixing-based systems. A unique IBE scheme [20] that is not always apparent to pairings was created by Boneh et al. Because to the quadratic residue problem, Cocks' technique is advised despite poor encryptions to maintain its mileage. Given the fast expansion of flexible cloud services in today's dispersed digital environment, data sharing utilising private clouds appears to be more impractical. IBE sets apart public key and assertion management at the PKI and is a crucial PKI goal. The additional calculation needed at the PKG during client disavowal poses a production risk for IBE, though. Understanding the project is crucial since sharing sensitive data through cloud services makes it challenging to provide comprehensive lifecycle strong security.

III. PROPOSED SYSTEM

Centralized management, visibility, as well as control are offered by a cloud-based access control system without the expense and complexity of conventional physical access systems. Systems like the Kisi software have true updates, internet wiring, diagnostics, and many other features. Without expensive certificates, proprietary command-line interfaces, or training, they may be installed quickly. One of the crucial security measures in cloud technology is access control. Data controllers can embed data access controls within the encrypted data thanks to attribute-based access control's adaptable methodology. The exploration of temporal aspects in determining and enforcing a data landlord's policies as well as the information user's privileges in cloud-based systems, however, has not received much attention. Traditional classifications of access control models include three categories: (1) Discretionary; (2) Mandatory; and (3) Role-based. Inside the discretion access (DAC) model, the object's owner determines and sets the access privileges for other users. A well-known illustration of the discretionary access control approach is the UNIX operating system. For instance, the subject (the owner of the object) may declare the permissions (read, write, and execute) that individuals within the same group and all other individuals may have. The modern multi-user as well as multi-application environment, a feature of distributed systems like the cloud, will result in significant administration overhead for DAC models, which are typically only employed with legacy apps. In our system paradigm, the enforcement of access controls depends solely on client-side periodic attribute matches between cypher texts and private keys. Cloud hosting does not need any user information that is needed to implement access policies in the re-encryption process. Because of this, this approach guarantees that privacy information, including user identification and access privileges in the user's encryption key, will not be revealed to cloud. Public cloud is a young field whose use is on the rise by many IT giant firms, including Salesforce.com, IBM, and Google.com. It combines a variety of technologies—utility computers, computation, virtualization, etc.—and takes advantage of their strengths to offer a number of advantages, including low upfront costs, enough storage, quicker calculations, virtualization, etc. Users can access personal data and information from any location at any time by storing it and sharing it in the cloud. One of key benefits of cloud is that individuals and organizations can pay as they go for access to the cloud's many resources, including storage, network, processing power, etc. Particularly those organisations that are unable to invest a substantial sum of money on infrastructure would benefit from this. As a result, there is a serious risk to a security of the cloud-based outsourcing of data. Additionally, since the owners of the data and the providers of Internet services are probably available in several jurisdictions, protection must be offered against these dubious providers. Regarding privacy and safety of the user's data are ensured by the individual security procedures built into all of these technologies. However, public cloud as a whole cannot use the security feature of one platform.

a) Framework

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

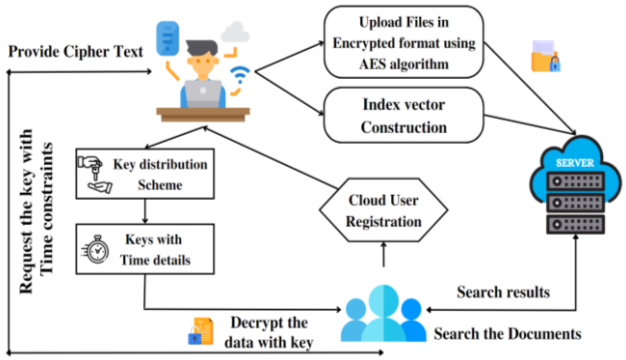

Fig. 2 Proposed System Framework

1) Data Sharing Framework

Our proposed solution, which combines two state-of-the-art cryptographic techniques, creates a scalable and accurate access control system for outsourced time-sensitive data. Time Limited Access Control and Elliptic Curve Cryptography. ECC plays a crucial role in implementing the timed-release feature and offering a flexible entry control primitive with predefined attribute sets. The framework involves the participation of the data owner, cloud provider, and data user processes.

2) Data Owner Register

In order to utilize this cloud application, data owners must register. Process registration is regarded as cloud access authorization. Information about registered users is sent to the provider. The request can be approved or denied by the service provider. Then, access to the cloud is granted to the approved users. Owners of registered data may log in and upload files using a specific user name and password.

3) Data / File Uploading

A registered owner has the privilege to upload files to the cloud. Before uploading, the files are encrypted using the CP-ABE algorithm. The file may be encrypted in accordance with the chosen policy before being uploaded to the cloud at the owner's option depending on particular attribute settings. In addition, the owner can establish one or more time points for each file to grant time-based access permission.

4) User Request for File Access

Users of data should register before accessing the cloud. They can access the cloud once their registration is complete. Users who have registered may search for and download files from the cloud. The particular data owner receives a request from the user when they want to view a file.

5) Time Control based Key Sharing

Users were given access restrictions by the data owner. Owners specified the pre - emotively for viewing the file when receiving the user's request. The server will then distribute the secret key to the requesting user. This sharing secret key is only valid for a specific amount of time. Otherwise, accessing the file will be indicated as invalid.

6) Data / File Access

The proposed TAFC system can facilitate an accurate and timed-release access control mechanism. This system allows access to the data by a single individual with a satisfied attribute set after the designated time period has elapsed. In the proposed scheme, users attempting to access data before the designated release time, even with a satisfying attribute set, are deemed compromised.

b) Comparison Table

1) Key Generation Time

The effectiveness of the proposed method was assessed by measuring the key generation time for different bit sizes. The results of a comparison between the suggested system and the current approach showed that the proposed system performs noticeably better than the current method. One illustration of this was a chart contrasting the two systems.

Table 1. Key Generation Time (MS)

Public Key	
08 - Bit	48
16 - Bit	32

2) Encryption and Decryption Time

The graph below displays the performance ratings of the present and recommended approaches based on encryption and decryption times. The suggested approach greatly outperformed the current technique when the two systems were compared, according to the findings. This was shown in a graph that contrasted the effectiveness of the two systems.

Table 2. Encryption and Decryption Time (MS)

Data Size	Existing	Proposed
1000 (1 GB)	19	7
2000 (2 GB)	24	11
3000 (3 GB)	33	17
4000 (4 GB)	39	25
5000 (5 GB)	44	31

IV. RESULT COMPARISON AND DISCUSSION

The proposed cloud environment includes a server, data owner, and data user entities. The server admin logs in using their unique ID and password. Users and data owners must register and wait for server approval before accessing the system. Once approved, they can change their information. The login process verifies the user's or owner's validity with their username and password. Owners can view

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181, [5] Vol. 12 Issue 08, August-2023

their registered details in the View Personal Information module. The file uploading process allows data owners to upload their encrypted files for sharing and storage on the server. Cloud computing has become a popular option for organizations to store and manage their data, but privacy and security concerns still exist. With resources being distributed among multiple clients, there is a risk of eavesdropping and unethical behavior. Dependence on cloud service providers also means trusting them with sensitive data, which can be vulnerable to manipulation by the data administrator. While smaller organizations may benefit from the safety of cloud providers, larger organizations may find them insufficient for protecting trade secrets and other classified information [1][16]. In 2008, The Linkup, a cloud provider with over 20,000 paying clients, experienced a system meltdown resulting in the loss of most of their customers' data. The company ultimately went out of business and blamed their storage partner for the failure. In 2009, an online bookmarking company suffered a similar data failure, resulting in the complete loss of customer bookmarks [18].

V. CONCLUSION

This framework offers time-sensitive data in the cloud storage fine-grained access control. Getting flexible scheduled release with fine resolution with lightweight overhead at the same time is a difficulty that hasn't been well investigated in previous research. The architecture of cipher text policy essential element encryption is smoothly integrated into the proposed scheme's timed-release encryption concept. In line with a well-defined access control method managing characteristics and release time, this strategy allows data owners the ability to flexibly distribute the allowed access to diverse individuals at various times. According to the research, our strategy can preserve the privacy of time-sensitive data while putting the least amount of strain possible on the server and data owners. Thus, it is a good fit for the real-world, extensive access control mechanism for cloud storage. Here, access control policy architecture for all conceivable time-sensitive access requirements is further investigated. This is done by strategically placing time trapdoors.

REFERENCES

[1] Wu, Xianglong, Rui Jiang, and Bharat Bhargava. "On the security of data access control for multiauthority cloud storage systems." IEEE Transactions on Services Computing 10.2 (2017): 258-272.

[2] Kolhar, Manjur, Mosleh M. Abu-Alhaj, and Saied M. Abd El-atty. "Cloud Data Auditing Techniques with a Focus on Privacy and Security." IEEE Security & Privacy 15.1 (2017): 42-51.

[3] Liu, Joseph K., et al. "Two-factor data security protection mechanism for cloud storage system." IEEE Transactions on Computers 65.6 (2016): 1992-2004.

[4] Cui, Baojiang, Zheli Liu, and Lingyu Wang. "Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage." IEEE Transactions on computers 65.8 (2016): 2374-2385.

[5] Zhu, Zhongma, and Rui Jiang. "A secure anti-collusion data sharing scheme for dynamic groups in the cloud." IEEE Transactions on parallel and distributed systems 27.1 (2016): 40-50.

[6] B. Zhang, J. Wang, K. Ren, and C. Wang, “Privacy assured Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166–177, Jul. Dec. 2013 outsourcing of image reconstruction service in cloud,” IEEE.

[7] B. Zhang, J. Wang, K. Ren, and C. Wang, “Privacyassured outsourcing of image reconstruction service in cloud,” IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166–177, Jul./Dec. 2013.

[8] R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” in Advances in Cryptology (EUROCRYPT‟03),E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646

[9] D. Boneh and X. Boyen, “Efficient selective-id secure identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT‟04), C. Cachin and J. Camenisch, Eds. Berlin,Germany: Springer, 2004, vol. 3027, pp. 223–238.

[10] D. Boneh and X. Boyen, “Secure identity based encryption without random oracles,” in Advances in Cryptology (CRYPTO‟04),M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206.

[11] B. Waters, “Efficient identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT‟05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.

[12] C. Gentry, “Practical identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT‟06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC‟08), 2008, pp. 197–206.

[14] S. Agrawal, D. Boneh, and X. Boyen, “Efficient lattice (h)ibe in the standard model,” in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.

[15] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, “Identity-based hierarchical strongly key-insulated encryption and its application,” in Advances in Cryptology (ASIACRYPT‟05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.

[16] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology (CRYPTO), G. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.

[17] C. Cocks, “An identity based encryption scheme based on quadratic residues,” in Cryptography and Coding, B. Honary, Ed. Berlin/ Heidelberg: Springer, 2001, vol. 2260, pp. 360–363.

[18] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, “Bonsai trees, or how to delegate a lattice basis,” in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010,vol. 6110, pp. 523–552.

[19] D. Boneh, X. Ding, G. Tsudik, and C. Wong, “A method for fast revocation of public key certificates and security capabilities,” in Proc. 10th USENIX Security Symp., 2001, pp. 297–308.

[20] B. Libert and J.-J. Quisquater, “Efficient revocation and threshold pairing based cryptosystems,” in Proc. 22nd Annu. Symp. Principles Distrib. Comput., 2003, pp. 163–171.

A.V.M.B. ARUNA is an esteemed assistant professor in the Department of Computer Science and Engineering at Periyar Maniammai Institute of Science & Technology, located in Tamilnadu, India. She is a highly accomplished individual, having been awarded a gold medal in her Master's Degree M.Tech Software Engineering, showcasing her expertise in the field of cloud computing. As a Project Coordinator for the final year, Aruna consistently demonstrates her passion for the subject and her commitment to academic excellence, which is reflected in her valuable

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

contributions to cloud computing research and education. Her dedication and proficiency make her a valuable asset to the realm of cloud computing.

M. R. SANTHOOSH is an aspiring B.Tech CSE student at Periyar Maniammai Institute of Science & Technology, Tamil Nadu, India, displaying profound interest in Cloud Computing. He actively engages in diverse academic and extracurricular endeavors, having assumed roles such as Executive Committee Member for the Energy and Environment Club (2021 - 22), Student Admission Coordinator in the academic year of (2020 - 21), and Department Advisory Committee Member (2021 - 23) in the Department of Computer Science & Engineering, making valuable contributions to curriculum and syllabus development.

A. RAJA RAJESWARAN is a dedicated B.Tech CSE student at Periyar Maniammai Institute of Science & Technology, Tamil Nadu, India. His keen interest lies in Cloud Computing, and he actively engages in exploring the latest developments in this domain.

A. SHARUK MOHAMED, a B.Tech CSE student at Periyar Maniammai Institute of Science & Technology, Tamil Nadu, India, is enthusiastic about Cloud Computing. He is driven by a curiosity to unravel the potential of cloud technologies.

G. RANJITH, a student at Periyar Maniammai Institute of Science & Technology in Tamil Nadu, India. His primary interest lies in the dynamic realm of Cloud Computing. Throughout his academic journey, he is driven by a strong determination to actively contribute to the continuous advancements in this field. Notably, Ranjith holds the prestigious rank of Corporal (CPL) in the National Cadet Corps (NCC), demonstrating his commitment to discipline and leadership. With his passion, dedication, and leadership abilities, he aspires to excel in Cloud Computing and make a positive impact on the industry's future.