A Biometric-Based Encryption Method for Secure Data Sharing in Cloud Environment

Gauraangi Praakash[1], Pooja Khanna[1], Sachin Kumar[1], Pragya[2]
[1]*Amity University Uttar Pradesh, Lucknow Campus,*
[2]*MVD College, University of Lucknow, Lucknow.*

Abstract

When seen from the point of view of information collecting, distributed storage can very easily be converted into a decision-making approach. In a short amount of time, data storage evolves into a technique of preference. Since data is protected remotely rather than locally, consumers from both the home and the technical sphere are inclined to do so. If the dispersed storage is not completely confident, it means that users have "the possibility to incorporate knowledge about the online cloud." Regardless of whether customers find cloud-based information to be a major cause for concern, the fact remains that it can be a difficult problem, especially because we trade data on cloud servers. To address this issue in a competent and effective manner, the Revocable IBE conspires, and the primary refreshing technique are both already available. In addition, cloud architecture experience needs to be improved to enable the utilization of contemporary safe information structures in distributed computing. In this sense, a figure (or any encoded document) can contain a temporary amount of time. If the characteristics of the figurative content fit the configuration of the key, and if all possible occurrences are permitted to take place, then the figurative content must be decrypted. After a client has specified an end time, the information is permanently removed from the cloud server in a secure manner. The framework proposed is equipped with features such as unfailing viability for both PKG measures and client shared secret key size because of the utilization of the key updating service that is made available by the cloud server, further the time comparison establishes that proposed technique with GSP is more efficient as compared to without GSP. Results show that the proposed system with GSP reduces processing time by approximately 0.001 times.

Keywords

Cloud Computing, Privacy Preservation, Bio-metric, Identity Based Encryption (IBE), Self-Destruction, Revocation.

1. Introduction

The most generally acknowledged example of distributed computing is the use of specialized properties or hardware that reside on re-bit computers as administration and is transferred on to the end user, with the internet being the most accepted example. Fame and significance are easily acquired by distributed storage. To safely exchange information, the identity-based encoding strategy or the use of identity mixes is used [2]. A remarkable cornerstone of cryptography is Identity Based Encryption. It's a kind of transparent key encryption where customers are a key to the personality of a customer (e.g., the email address of a customer) because there are certain special specifics about it. To enter the general population criteria of this scheme, a sender must be able to encrypt a message using the contents measurement of the recipient's email address. The beneficiary collects her scrambling key from a specialist who can be trusted because he manufactures mystery keys for every client. It offers every conference an opportunity to enjoy the perceived character and an open key. The Private Key Generator is a trusting outsider's private key [13-15] The PKG key not only maintains the proportional ace private

International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT 2023), May XX-XX, 2023, Delhi, India

EMAIL: gauraangi.praakash@s.amity.edu(G. Praakash); pkhanna@lko.amity.edu(P.Khanna); skumar3@lko.amity.edu(S.Kumar), dr.pragya2011@gmail.com(Pragya)
ORCID: 0009-0008-3814-6247 (G. Praakash); 0000-0002-0043-1068 (P.Khanna); 0000-0003-2196-4573 (S.Kumar) ;0000-0002-5569-0307 (Pragya)

key but also disseminates an ace open key for the programmed to run. Every participant will be able to calculate an open key that is somewhat near to the personality ID if they enter the ace open key alongside the character respect given by the ace open key. The PKG, which utilizes the ace encryption key to render the private key for character ID, relates to the meeting that approved using the character ID to receive a coordinating private key. This allows the PKG to render the private key for personality ID. For security purposes, whether a client exits the meeting or acts poorly, he or she must be expelled from the gathering. This disavowed customer should then never have the right to get to and alter exchanged information again. A. Boldyreva, et al. [3] a revocable Identity Based Encryption scheme has been proposed, but it has the drawback of requiring calculation at a single level, i.e., an administrator or important individual from the organization. An estimation of outsourcing into IBE renunciation has been offered as a means of addressing this problem. Framework suggests a way for dumping all key era- related forms that must be completed between the key-issuing and key-refreshing processes. This would leave PKG and eligible clients with only a few straightforward activities to carry out locally. Another technique for the issuance of safe keys is suggested, and this one uses a half-breed private key for each customer. In addition, an AND gate is incorporated into the process of determining the key's age, and this gate is directed especially to the personality component and the time segment.

Similarly, in distributed computing, a stable information self-destructing system is proposed to increase distributed storage space. Each ciphertext in this structure is named with a time between value, so the private key is associated with a duration moment. The moment and the ciphertext will follow the key will be extracted if both the time characters and its related characters are present in the dictionary. In general, the owner has the authority to determine whether specific confidential data is valid for a given duration, i.e., whether it self-destructs at the end of a time span specified by the owner, or whether it cannot be released before a specific deadline.

2. RELATED WORK

The creator proposes a fully realistic encryption plot based on personalities in this paper [4] (IBE). In the arbitrary prophet display, the structure has chosen ciphertext defense, anticipating the Diffie-Hellman problem in a different computational form. The framework concentrates on logarithmic mapping linking the groups. Weil's fusion with elliptical curves is a consequence of this kind of principle. An alternative Concept of an open key encryption is introduced by the author in study presented in [3] called as Identity based encryption. It is more efficient and popular as it does not require the standard public key infrastructure for key management. Any environment, whether based on PKI or personality, must provide a way for customers to leave the system. Capable disavowal is a frequently discussed topic in the standard PKI environment.

On the other hand, there hasn't been much work done in the IBE environment to concentrate on the components of denial. When scrambling, the arrangement that is the most grounded demands that senders continue to employ eras and that collectors routinely update respective encryption information by meeting with a reliable specialist. In any event, this setup does not scale very well; when the number of users increases, the function upon that main page becomes a bottleneck, and the configuration does not scale very well. We propose a conspiracy including the IBE that would considerably increase the suitability of key-refresh in favor of the stock that is placed in collection while continuing to retain the capability of supplying the customers.

Our structure has been shown to be secure, and it is derived from the ideas behind the information structure of the primitive and double trees used in the fuzzy IBE. The author of [5] focused on a variant of Identity-Based Encryption (IBE) that is referred to as Fuzzy Based Identity Encryption. Within the framework of Fuzzy IBE, a lifestyle is characterized by a collection of illustrative characteristics. A private key is used in a Fuzzy IBE arrangement to transcribe a figure material along with an identification for an identity, Providing, and only providing, that the characters are! In addition, according to the results of the partition measure known as "set cover," 0 and 0 are the same.

What precisely considers air conditioning number is a characteristic of a Fuzzy IBE plan referred to as its screw- up resistance. The usage of biometric identities, which will be permanently disrupted each time they are evaluated; the "mess up resistance property" of the Fuzzy IBE plan is simply what considers the air conditioning number as a factor. the utilization of biometric identities, which will invariably result in the production of some sort of disturbance each time that they are evaluated; the defect tolerance characteristic of a fuzzy IBE plan is precisely what takes into consideration air conditioning number [17-21]. The utilization of several types of biometric IDs as required in addition, we show how the Fuzzy-IBE algorithm can be used for "quality-based encryption," which is a concept that we define.

The creator tackles the dilemma of using untrusted (conceivably harmful) cryptographic accomplices in this paper [6]. Here, to ensure the privacy of the data outsourced over cloud, a structured mechanism has been proposed. In this model, the organized state of the will shapes the item for the accomplice, but as the contraption begins to depend on it, there is no synchronization correspondence with it. Not only does it offer a process for calculating adequacy and testing the potential of an outsourcing use, but it also provides a mechanism for measuring the adequacy. It also involves two simple stable outsourcing deals. It demonstrates how to outsource computed exponentiation, which is the technological limitation in most open encryption algorithms on computationally limited computers, in a secure manner. A computer will require O (n) special increases if it is to complete exponentiation frame bit types if it does not make use of outsourcing. Any exponentiation-based scheme in which the authentic contraption can employ two untrusted exponentiation programs as measurements, and with which use the Cramer-Shoup cryptographic algorithm and Schnor checks causes the pile to decrease to O (log2 n). Using an untrusted Cramer-Shoup encryption program, we achieve a comparable weight reduction for a simple going considered security for another CCA2-secure encryption arrangement.

As shown by the author in this paper [7], attribute-based encryption (ABE) is a promising cryptographic standard instrument for fine-grained access control. However, in current ABE schemes, the computational approach to online encryption often results in a one-sided life of access course of action, which translates into an obstacle to its use. In this article, a novel approach for outsourcing ABE encryption to a cloud organization provider is proposed to reduce the awkwardness of group computation. It makes use of an improved Map. Reduce cloud advancement by ensuring that at least one of the slave center points is visible from the master center point and, moreover. After outsourcing, the customer will experience an accurate numerical loss that is decreased from the initial loss of four exponentiations during the encryption process to a hazy four exponentiations. Another potential drawback of the change that is being suggested is that the customer may opt to encrypt each action.

The migration of data from a company's local servers to those hosted in the cloud can be accomplished with the help of cloud-based data clients. The result of this is that the consumer is relieved of the cost of maintenance while also receiving data storage facilities of a high grade. The use of cloud storage creates a lot of privacy and safety concerns. Both the companies that supply cloud services and the servers that store data have some shortcomings. Concerns have been raised by the customer over the integrity of the data that has been uploaded to cloud storage. In this piece, the public key hash algorithm is utilized. In addition, for data dynamics, this makes it easier to do dynamic operations such as inserting new data, updating existing data, removing old data, and altering blocks.

The Merkle Hash Tree [8] is a tool that is utilized to help in the process of finding the position of each complex operation. A third-party examiner validates the accuracy of the user's data and attests to the reliability of the information that is kept on the cloud server. There is a significant reduction in the amount of computational and communication overhead. The defragmentation method is utilized to ascertain whether the file in question already resides on the cloud server before the user uploads it to the cloud storage location of their choice. This solution is robust and secure, even when faced with malicious server-launched replace attacks.

According to the author of this paper [9], ABE is an insight into future architecture that has mostly been associated with application fine-grained access control systems. However, as the numerical expense rises due to the multifaceted nature of the get-to recipe, ABE's high scheme over-head is being scrutinized. Since they have forced the figuring of assets, this problem has proven to be more genuine for portable de- indecencies. It demonstrates a general and capable approach for integrating a quality-based access management framework into ABE by introducing secure outsourcing strategies to achieve the aforementioned goal. More specifically, two cloud specialist co-ops (CSPs) have been created, namely the key age cloud specialist co-op (KG-CSP) and the decryption cloud specialist co-op (D-CSP), to handle outsourced key- issuing and unscrambling independently for the benefit of trait specialists and consumers.

In author in study [10], presented the automated formulation of cryptographic system for forward security. Mystery keys are refreshed on a regular basis; contact with a mystery key coordinating to a specific day and age does not allow a challenger in a forward-secure schedule to "kill" some previous period's strategy. Forward-secure advanced label plans, key-trade conventions, and symmetric-key plans have all seen developments. Under the definitive bilinear assumption of Diffie-Hellman, the primary building achieves security close to chosen plaintext attacks in the standard model. This structure is intuitive, and as the total number of eras grows, all parameters evolve in a logarithmic fashion.

3. IMPLEMENTATION DETAILS

With recent development in storage and technical advancements, cloud computing has stepped in as universal solution with features like colossal size data storage, bulky calculation, low-value benefit, and adaptable approach to get to the data. Concept is based on ide of virtualization. Virtualization is targeted to incorporate set of virtual assets or devices like storage gadget, server, organize or working system where the structure partitions the space into sectors to match the exact number of execution conditions that are required. Cloud computing is a powerful technique to for management of storage issues and insides of its administration, model suggested provides the data owner the capability to outsource and keep files saved at cloud platform. Number of organizations and subscribers have started employing cloud storage as reliable and easy to access source for facilitating data administration, processing, and storage, though concerns of security and privacy do exist. One of the primary concerns is whether the data stored in reliable manner and will not go missing in cloud facility.

Issues related whether organizations managing cloud facility meets data safety requirement of the client is a major concern. Concerns altogether make it vital and important to increase the confidence of data owners on cloud facility. Diversified models exist for securing and processing of data for public domain model and private domain model. Generally, with Private domain model, the owner of the data can establish the fidelity of the outsourced data that is being managed and stored at the cloud facility.

In this technique, the owner of the outsourced data is supposed to have expertise. One more major concern happens to be integrity and authenticity of the security mechanism taking care of steps related to accessing the data. Numerous methods exist for key generation, traditional mechanism employed for encryption is not enough for countering the attack techniques deployed by the unauthorized users and attackers. For aforementioned reasons an encryption technique based on user feature can be a efficient method for enhancing security. Technique offers a unique key based on a user feature; this technique can make the data access very secured but there is definitely there is scope for error if not security. Further an innovative solution could be to employ hybrid technique of a feature-based mechanism in tandem with user biometric data i.e. fingerprint, iris, face features etc. to improvise the system and secure the data access with unauthorized access nearly impossible. Employing to much in-between steps on the security concerns and including the resolution for the minutest detail may lead to the degradation in the efficiency of the system. Therefore, a balance is to be maintained for improving the security measures and efficiency acceptable. [22-25]

The proposed architecture and implementation details of the system has been discussed in this section. Following figure 1 shows the schematic representation of the proposed system.

A. System Overview

The client builds an account on the cloud and then logs in to frameworks using a correct username and password. User demands KU-CSP keys [1] after signing in. The client / proprietor uses the keys to scratch the documents and move them to the cloud server over a fixed period, all while being completely weightless. The remaining client is then sent to the KU-CSP, which creates a new key or refreshes the old ones in order to keep the device secure and passes the new keys to the client's key. The residual consumer is reshaped at this stage. When the predefined document cycle on the cloud server is complete, the report will be lost to the server and will no longer be available to clients. The computing space of the cloud system is expanded as a result of this. To overcome the disadvantage of the previous framework, the framework genius postures information self-destruction strategy. The literature review shows that the existing mechanism retains the data as it is over the cloud storage, even if it is no longer in use. It makes the users, remove the data manually to free the space. Thus increasing the workload of the user and simultaneously occupying the storage unnecessarily over the cloud storage. Thus, to overcome these issues from the existing system, our proposed system has the mechanism to automatically destroy the data once either the time duration to access the data is over or the data is no longer needed. We call this feature as self-data destruction mechanism. Here, the information is transmitted to the cloud server for a set period (for example, (2/2/2023-3/2/2023,). Here, in this example the data outsourced over cloud will be accessible to the authorized user only for the specified time frame of a day. Once the permissible time frame is over, the system will revoke the accessibility and destroy the data from the server. It will ensure the security of the data from unauthorized access also it will free the space from the server.

B. Data Self-Destructing Mechanism

A Self-Destructing Scheme known as key-strategy personality-based encryption collaborates with time-defined characteristics, which is based on the review that each identification thing can be linked to an arrangement of properties in suitable cloud application circumstances, and each attribute is linked to a time interval detail, demonstrating that the encrypted data thing can be deciphered between those periods. Each user's key is linked to a get-to tree, and each leaf hub is linked to a period during which the data owner scrambles his or her information before distributing the device to customers. Since the get to tree's simple articulation can mean any desired information index for it, it can obtain fine- grained get to command at any time between each of the. The ciphertext cannot be decoded if the time moments are not within the predefined time intermediate, i.e., the ciphertext will be naturally lost and no one would be able to unscramble it due to the secure key closure. Along these lines, it is possible to achieve a secure self-pulverization of data with fine-grained control. The essential characteristics should satisfy the get to tree, where even the time span of each leaf in the key customers should have a place in the ciphertext with the coordinating characteristic, keeping in mind the goal of effectively unscrambling the ciphertext.

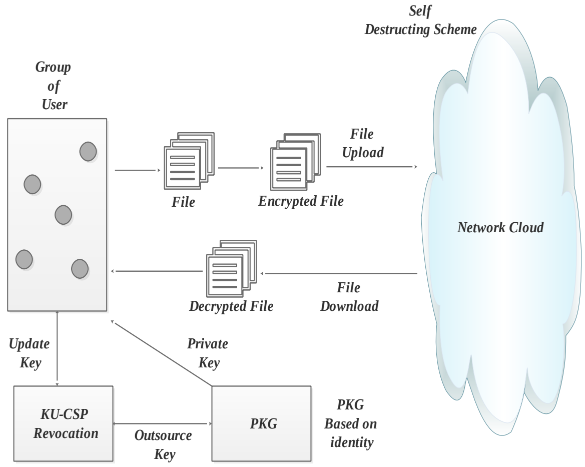


Figure 1: System Architecture

C. Experimental Setup

The IDE tool for the development of the system is NetBeans 8.1 and JDK 1.8 were included in the system as a front end on the Windows level. The program can be run on any regular computer. The system would not have to think about running a specific machinery.

4. ALGORITHM FORMULATION

In a short amount of time, data storage evolves into a technique of preference. Since data is protected remotely rather than locally, consumers from both the home and the technical sphere are inclined to do so. If the dispersed storage is not completely confident, it means that users have "the possibility to incorporate knowledge about the online cloud."

Regardless of whether customers find cloud-based information to be a major cause for concern, the fact remains that it can be a difficult problem, especially because we trade data on cloud servers.

Assume S represents the system where.

S = {Φ, KDC, CS}

Table 1

Algorithm – Biometric based Encryption

i. User

Φ = {Ṝ, £, ¥, €, δ} Where,

Ṝ= User Registration

£= User Login

¥= Request for Key

€= Encryption of

Data δ= User

Revocation

ii. Key Distribution Centre KDC= {α, β}

Generating set of Keys

α= {α1, α2, α3 ... αn}

Where α represents the set of public keys.

β= {β1, β2, β3 ... βn}

Where β represents the set of private keys generated with respect
to the public key.

iii. Cloud Server is CS: {U, D} ;

D: {F, T}

where

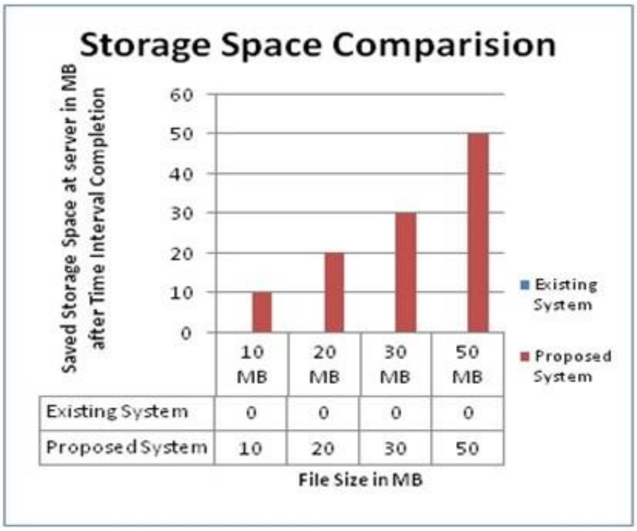
U: File to be Uploaded

D: the process of self-destruction

F: Number of files

T: Time Interval

To address this issue in a competent and effective manner, the Revocable IBE conspires, and the primary refreshing technique are both already available. In addition, cloud architecture experience needs to be improved to enable the utilization of contemporary safe information structures in distributed computing. In this sense, a figure (or any encoded document) can contain a temporary amount of time. If the characteristics of the figurative content fit the configuration of the key, and if all possible occurrences are permitted to take place, then the figurative content must be decrypted. After a client has specified an end time, the information is permanently removed from the cloud server in a secure mannerAn Example of equation.



	10 MB	20 MB	30 MB	50 MB
Existing System	0	0	0	0
Proposed System	10	20	30	50

Figure 2: Storage Space Comparison Graph

5. RESULT & DISCUSSION

The graph illustrates the difference between some of the system's storage space and the proposed storage space, the system has been unable to retrieve the data from the public cloud, but the constructed methodology will delete the data from the public cloud after a stated amount of time, minimizing the cloud server's storage space. The various files on the cloud server are shown in the x-axis, while the storage in the y-axis is stored in mb.

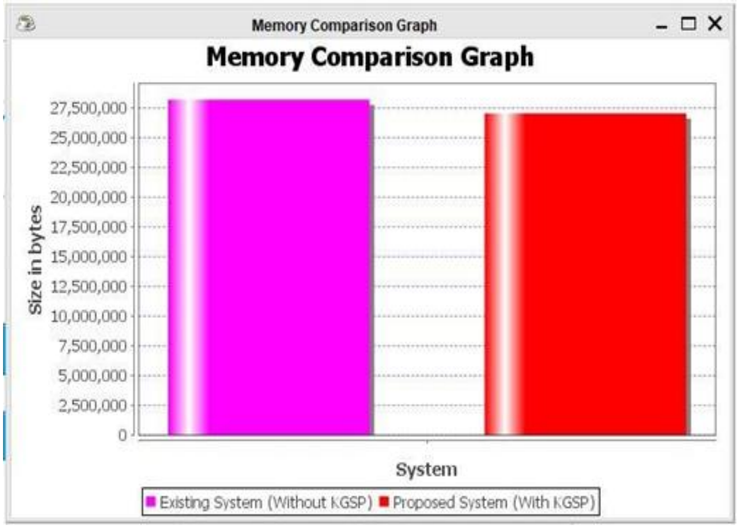


Figure 3: Memory Comparison

Figure 3 and 4 shows the comparison of space and time complexity of the system implemented with and without dedicated key distribution server. From the graph, implementation of dedicated key generation server reduces the complexity and make the system more efficient.

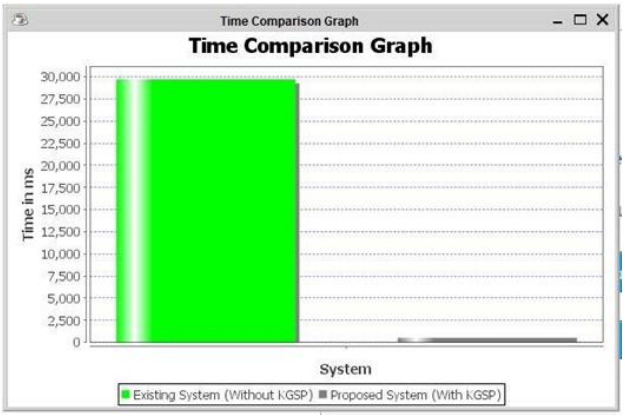


Figure 4: Storage Space Comparison Graph

6. CONCLUSION

The rapid expansion of flexible cloud administration has resulted in the emergence of several previously unanticipated issues. One of the most significant challenges is figuring out how to securely remove information that has been outsourced and stored in the cloud. This paper proposed an information self-destructing mechanism that can achieve the time defined ciphertext in distributed computing to resolve the issues. This mechanism would resolve the issues by performing an adaptable wonderful get to control between the consent specified time and moment self-decimation after coming close to shared and outsourced information. IBE is also familiar with the catch-22 situation that arises when a character is repudiated by an estimate that can be revocably outsourced. There is no need for a safe channel or client verification during the key updating process that takes place between the client and the KU-CSP. In addition, the framework is equipped with features such as unfailing viability for both PKG measures and client shared secret key size because of the utilization of the key updating service that is made available by the cloud server, further the time comparison establishes that proposed technique with GSP is more efficient as compared to without GSP. The framework proposed is equipped with features such as unfailing viability for both PKG measures and client shared secret key size because of the utilization of the key updating service that is made available by the cloud server, further the time comparison establishes that proposed technique with GSP is more efficient as compared to without GSP. Results show that the proposed system with GSP reduces processing time by approximately 0.001 times.

7. References

[1] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, “Identity-Based Encryption with Outsourced Revocation in Cloud Computing”, in IEEE transactions on computers, vol. 64, no. 2, february 2015.

[2] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,” In Advances in Cryptology CRYPTO98). New York, NY, USA:Springer, 1998, pp. 137-152.

[3] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. 15thACMConf. Comput. Commun.Security (CCS08), 2008, pp. 417-426.

[4] D. Boneh and M. Franklin, “Identity-based encryp-tion from the Weilpairing,” in Advances in Cryptology CRYPTO „01), J. Kilian, Ed.Berlin, Germany: Springer, 2001, vol. 2139, pp. 213-229.

[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,”in Advances in Cryptology (EUROCRYPT‟05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557-557.

[6] J. Li, C. Jia, J. Li, and X. Chen, “Outsourcing encryp-tion of attribute based encryption with mapreduce,” in Information and Communications Security. Berlin, Heidel-berg:Springer, 2012, vol. 7618, pp. 191-201.

[7] 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.

[8] R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.

[9] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, “Fine-grained access control system based on outsourced attribute-based encryption,” in Proc. 18th Eur. Symp. Res. Comput. Secu-rity (ESORICS), 2013,pp. 592-609.

[10] R. Canetti, S. Halevi, and J. Katz, “A forward-secure publickey Encryption scheme,” in Advances in Cryptology (EUROCRYPT'03), E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656,pp. 646-646.

[11] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” Nat. Inst. Stand. Technol., Tech. Rep. SP 800 - 145, 2011.

[12] C. Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2011, pp. 820–828.

[13] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” in Proc. 20th USENIX Conf. Security (SEC‟11), 2011, pp. 34–34.

[14] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, Identity-based hierarchical strongly key-insulated encryption and its application, in Advances in Cryptology (ASIACRYPT05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495 514.

[15] 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. 297308.

[16] B. Libert and J.-J. Quisquater, Efficient revocation and threshold pairing based cryptosystems, in Proc. 22nd Annu. Symp. Principles Distrib. Comput., 2003, pp. 163171.

[17] H. Lin, Z. Cao, Y. Fang, M. Zhou and H. Zhu, "How to design space efficient revocable IBE from non-monotonic ABE", Proc. 6th ACM Symp. Inf. Comput. Commun. Security (ASIACCS’11), pp. 381-385, 2011.

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

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

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

[21] P. Singh, P. Khanna and S. Kumar, "Communication Architecture for Vehicular Ad Hoc Networks, with Blockchain Security," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2020, pp. 68-72, doi: 10.1109/ICCAKM46823.2020.9051499.

[22] Gupta, A., Khanna, P., Kumar, S. (2021). A Hybrid Blockchain-Secured Elderly Healthcare Environment. In: Tanwar, S. (eds) Blockchain for 5G-Enabled IoT. Springer, Cham. https://doi.org/10.1007/978-3-030-67490-8_16

[23] Kumud Tiwari, Sachin Kumar, Pooja Khanna, Anil Kumar, "Blockchain-based transaction validation for patient interoperability in Healthcare 4.0", Blockchain Applications for Healthcare Informatics, Academic Press, 2022, Pages 1-26, ISBN 9780323906159, https://doi.org/10.1016/B978-0-323-90615-9.00017-7.

[24] Kumar, S., Khanna, P., Pragya, Tripathi, S. (2023). Biometric Assisted Multi-modal Encryption Key for Secured FHSS Communication. In: Bhattacharyya, S., Banerjee, J.S., Köppen, M. (eds)

Human-Centric Smart Computing. Smart Innovation, Systems and Technologies, vol 316. Springer, Singapore. https://doi.org/10.1007/978-981-19-5403-0_12

[25] S. Priya, G. Srivastava and S. Kumar, "Blockchain Integrated Crowdfunding Platform for Enhanced Secure Transactions," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), Noida, India, 2021, pp. 280-285, doi: 10.1109/RDCAPE52977.2021.9633380.