Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**

EMPOWERING SECURE GROUP DATA SHARING IN CLOUD COMPUTING THROUGH BLOCK DESIGN KEY AGREEMENT

#1 Mrs.S.LAVANYA, #2SK.RIZWANA, #3 Y.PRABHAS, #4 M.SHYAM, #5 CH.SRINADH
#1Assistant professor in Department of IT, DVR & Dr.HS MIC College of Technology,Kanchikacherla
#2#3#4#5 B.Tech with Specialization of Information Technology , DVR &
Dr.HS MIC College of Technology,Kanchikacherla-521180

Abstract_ Cloud computing data sharing enables two users to freely divide up the organization's records, which increases worker productivity in collaborative settings and has broad potential uses. Nonetheless, ensuring the security of information sharing inside a collection and appropriately allocating the outsourced records within a collection structure are challenging tasks. Keep in mind that important agreement protocols have played a vital role in stable and environmentally friendly institution record sharing in cloud computing.

.. In this paper, we present a unique block design-based total key agreement protocol that supports a pair of members and can dynamically expand the range of members in a cloud environment based on the block design's shape by utilising the symmetric balanced incomplete block design (SBIBD). We provide a well-liked formulation for generating the common place convention key K for a few individuals, based on the suggested institution data sharing model. It should be noted that by maximising the (v; k + 1; 1)-block design, the communiqué complexity is significantly lowered and the computational complexity of the suggested protocol will increase linearly with the range of members.

1.INTRODUCTION

Distributed computing and distributed storage became hotly debated issues in ongoing many years. Each is steadily changing the way we tend to live and enormously further developing creation power in certain areas. As of now, in view of limited stockpiling assets and furthermore the interest for helpful access, we tend to lean toward to store a wide range of data in cloud servers, that is moreover a respectable opportunities for firms and associations to keep away from the above of conveying and keeping up with gear when data is keep locally. The cloud server gives an open and advantageous stockpiling stage for individuals and associations; nonetheless, it furthermore presents security issues. For example, a cloud framework could likewise be exposed to assaults from each malevolent clients and cloud suppliers. In these situations, affirming the security of the hang on data inside the cloud is significant. In [1], [2], [3], many plans were projected to safeguard the security of the rethought information. The on top of plans exclusively considered security issues of a solitary data proprietor. Nonetheless, in certain applications, various information property holders might want to share their data during a group way immovably. In this manner, a convention that supports secure bunch data sharing under distributed computing is required. A key understanding convention is utilized to get a run of the mill gathering key for numerous members to affirm the security of their later correspondences, and this convention is applied in distributed computing to help secure and prudent data sharing. Since it totally was presented by Diffie-Hellman in their original paper [4], the key understanding convention has become one in everything about essential cryptographic natives. The key variant of the Diffie-Hellman convention gives a proficient goal to the question of making a typical mystery key between 2 members. In cryptography, a key understanding convention might be a convention inside which two or a great deal of gatherings can settle on a key in such the least difficult manner that each impact the result. By utilizing the key understanding convention, the conferees will solidly send and get messages from each other utilizing the normal meeting key that they concur upon ahead of time. In particular, a solid key understanding convention guarantees that the resister can't get the created key by executing malevolent assaults, like listening in. In this way, the key understanding convention is wide used in intelligent correspondence conditions with high security necessities (e.g., remote executive gatherings, video chats, helpful work areas, recurrence ID [5], distributed computing and afterward on). The Diffie-Hellman key arrangement [4] gives the easiest method for getting keys. In any case, it doesn't offer partner confirmation administration, which makes it in danger of principal the-center assaults. This case can be self-addressed by adding a few styles of confirmation instruments to the convention, as arranged by Regulation et al in [6]. Also, the Diffie-Hellman key understanding will exclusively uphold 2 members. Accordingly, to disentangle the different key assaults from pernicious conferees, who imagine to purposely postpone or obliterate the gathering, yi arranged partner character based issue lenient meeting key understanding in [7]. Presently, a few explores are given to raise the insurance and correspondence productivity of the key understanding convention, that is roofed inside the writing [8], [9], [10], [11]. Note that in Chung and

Base paper [12] and Lee et al. 's paper [13], block style is used inside the style of partner affordable burden balance algorithmic rule to keep up load adjusting in a really circulated framework. Propelled by [12] and [13], we will generally present the symmetric adjusted fragmented block style (SBIBD) in arranging the key understanding convention to downsize the nature of correspondence and calculation.

2.LITERATURE SURVEY

1. H. Yan, J. Li, and Y. Zhang, ‘‘Remote data checking with a designated verifier in cloud storage,’’ IEEE Syst. J., vol. 14, no. 2, pp. 1788–1797, Jun. 2020.

Abstract:

Remote data possession checking (RDPC) supplies an efficient manner to verify the integrity of the files stored in cloud storage. Public verification allows anyone to check the integrity of remote data so that it has a wider application in public cloud storage. Private verification just allows the data owner to verify the data integrity, which is mainly applied for the verification of secret data. However, in many real applications, the data owner expects a specific user to check the files in cloud storage, whereas others cannot execute such work. It is obvious that neither public verification nor private verification can satisfy such a requirement. To solve this issue, Ren et al. provided a designated-verifier provable data possession (DV-PDP) protocol. Unfortunately, the DV-PDP is insecure against replay attack launched by the malicious cloud server. To overcome this shortcoming, we present a new RDPC scheme with the designated verifier, in which the data owner specifies a unique verifier to check the data integrity. Based on the computational Diffie-Hellman assumption, we prove the security for our RDPC scheme in a random oracle model. The theoretical analysis and experiment results indicate that our scheme has less communication, storage, and computation overhead while achieving high error detection probability.

2. J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, ‘‘RKA security for identity-based signature scheme,’’ IEEE Access, vol. 8, pp. 17833–17841, 2020

Related-key attack (RKA) is a kind of side-channel attack considered for kinds of cryptographic primitives, such as public key encryption, digital signature, pseudorandom functions etc. However, we note that the RKA-security seems to be not considered for identity-based signature (IBS), which is an important primitive for identity-based cryptography and proposed by Shamir in 1984. In this paper, for the first time, we introduce the RKA security into IBS schemes and try to define the security model for it. More specifically, we consider the RKA occurs in the users’ signing key or the master key of the key-generation center (KGC), which derives two kinds of RKA securities for

IBS. Meanwhile, we illustrate that the most efficient Schnorr-like IBS scheme proposed by Galindo and Garcia is RKA-insecure by launching a simple RKA. However, a slight modification of it yields a RKA-secure IBS scheme, for which we give the detailed security proof in the random oracle. Finally, the performance analysis shows that the modified scheme is still extremely efficient but has higher security

3.PROPOSED SYSTEM

A key-agreement procedure in cryptography enables two or more parties to securely decide on a key, avoiding undesired third-party intervention. Using a Symmetric Balanced Incomplete Block Design (SBIBD), a group data sharing model is built to accommodate a group data sharing scheme for several members. The (v, k + 1, 1)-design, where v is the number of participants and blocks and each block has k + 1 people, is created using an algorithm. By guaranteeing participants' secure key agreement, the protocol improves the security of data sharing in cloud computing environments.

3.1 IMPLEMEMTATION

Members: are composed of a series of users based on the SBIBD communication model. In our scheme, members are people with the same interests (e.g., bidder, doctors, and businessmen) and they want to share data in the cloud. The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data. In our system, users of the same group conduct a key agreement

Cloud: provides users with seemingly unlimited storage services. In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services. However, the cloud has the characteristic of honest but curious. In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the user’s identity. The cloud is a semi-trusted party in our scheme.

2) Group Manager:

Group manager is responsible for generating system parameters, managing group members (i.e., uploading members’ encrypted data, authorizing group members, revealing the real identity of a member) and for the fault tolerance detection. The group manager in our scheme is a fully trusted third party to both the cloud and group members.

Firstly, users with the same interest register at the group manager so as to share data in the cloud. In addition, user revocation is also performed by the group manager. Secondly, all members of the group based on the SBIBD structure jointly negotiate a common session key, which can be used to encrypt or decrypt the outsourced data. Finally, when a dispute occurs, the group manager is able to reveal the real identity of the group member. Note that in our system model, data uploading and access control are performed by the group manager.

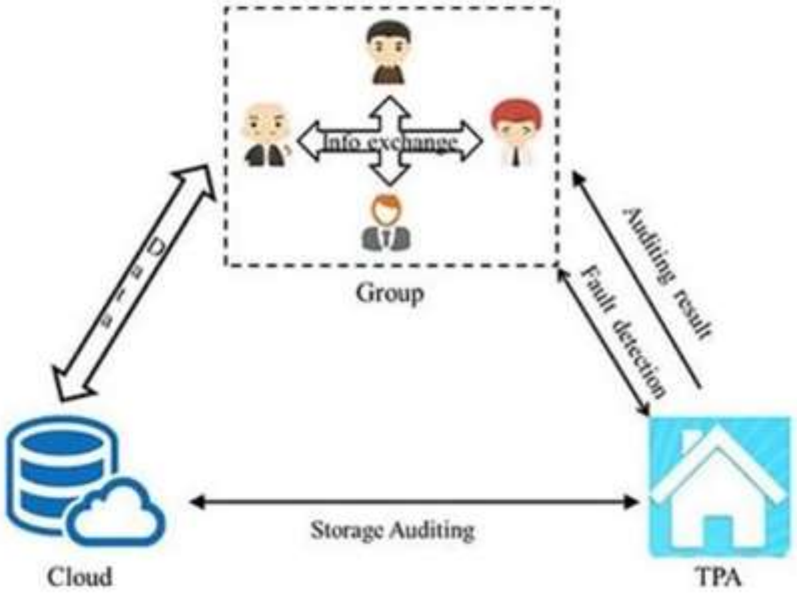
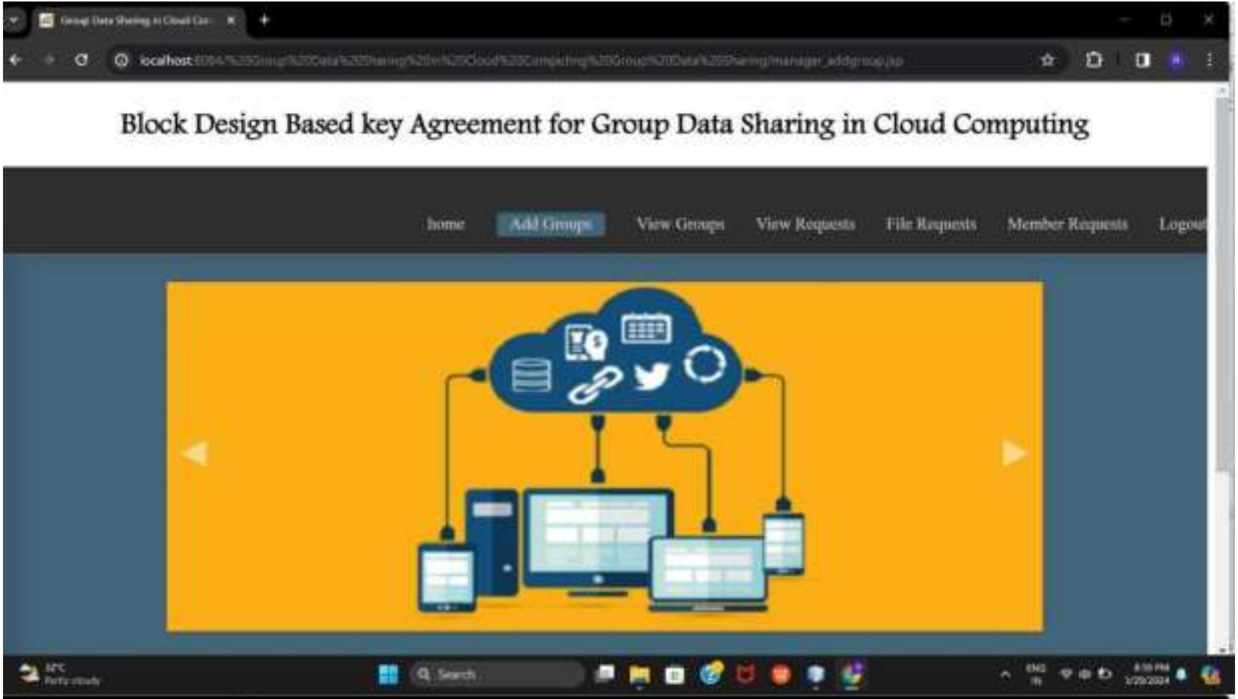
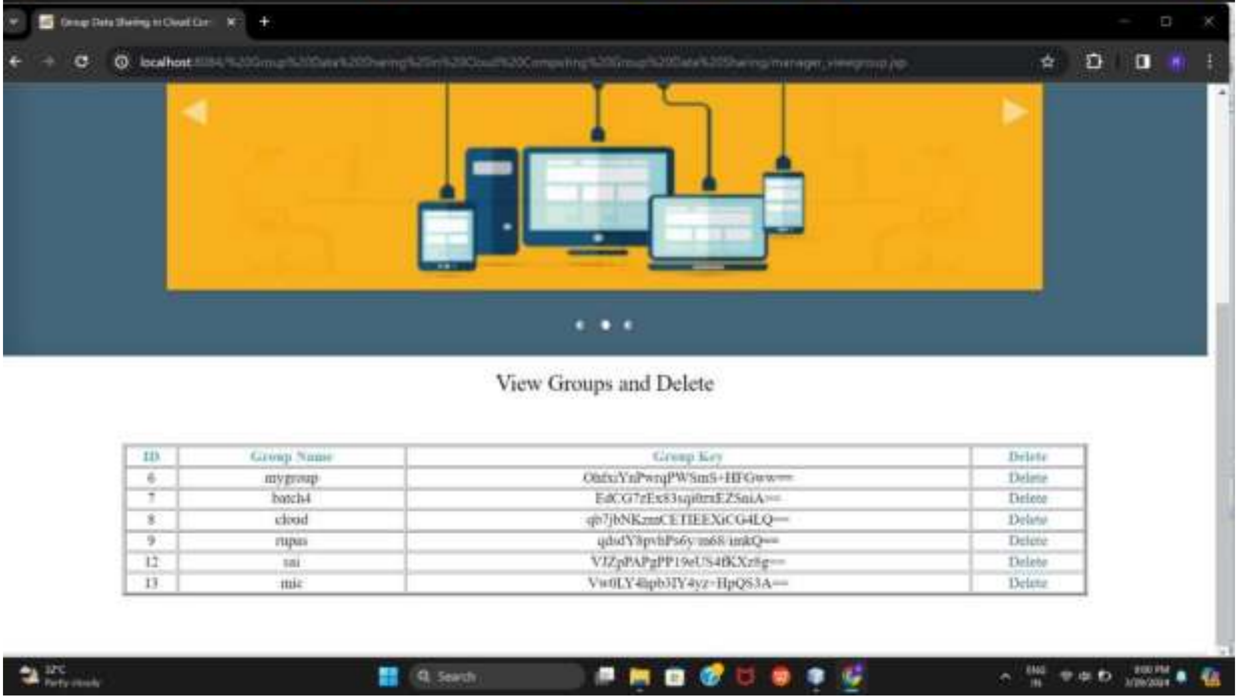


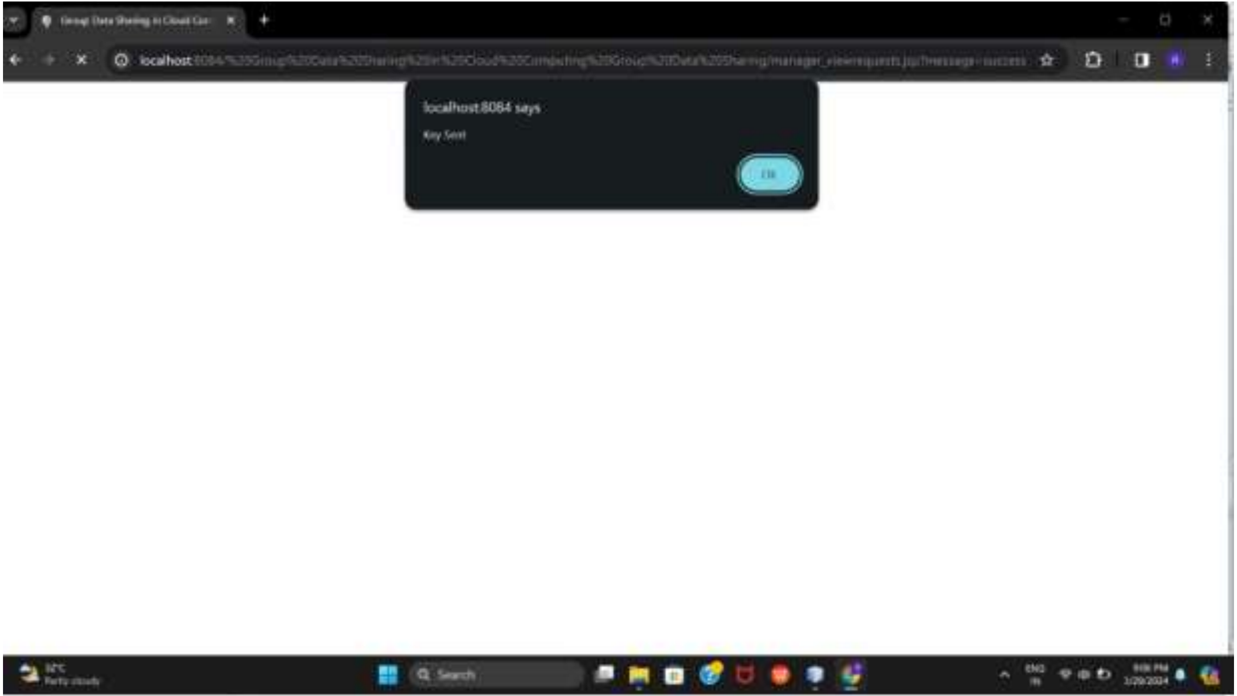
Figure 1 System Architecture

4.RESULTS AND DISCUSSION


Block Design Based key Agreement for Group Data Sharing in Cloud Computing

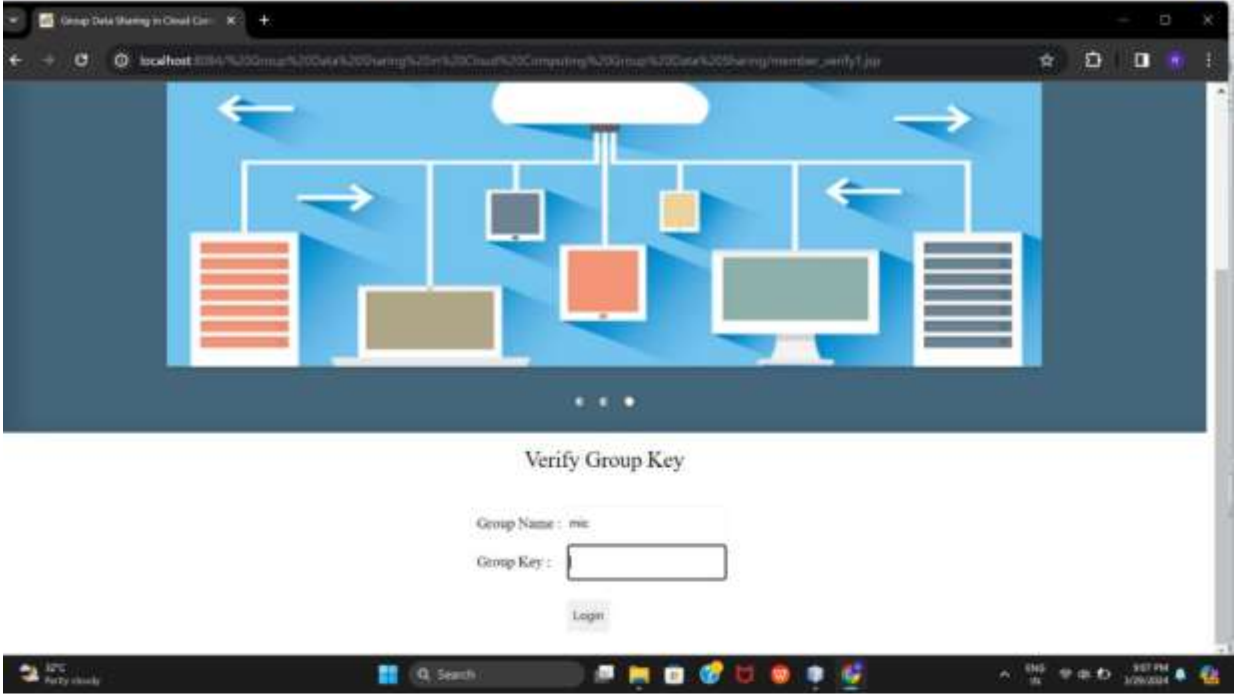

View Groups and Delete

ID	Group Name	Group Key	Delete
6	mygroup	OhfxiYnPwrqPWSmS+HFGww==	Delete
7	batch4	EdCG7zEx83sqi0rnEZSniA==	Delete
8	cloud	qb7jbNKzmCETIEEXiCG4LQ==	Delete
9	rupas	qdsdY8pvhPs6y/m68/imkQ==	Delete
12	sai	VJZpPAPgPP19eUS4fKXz8g==	Delete
13	mic	Vw0LY4hpb3IY4yz+HpQS3A==	Delete



localhost:8084 says

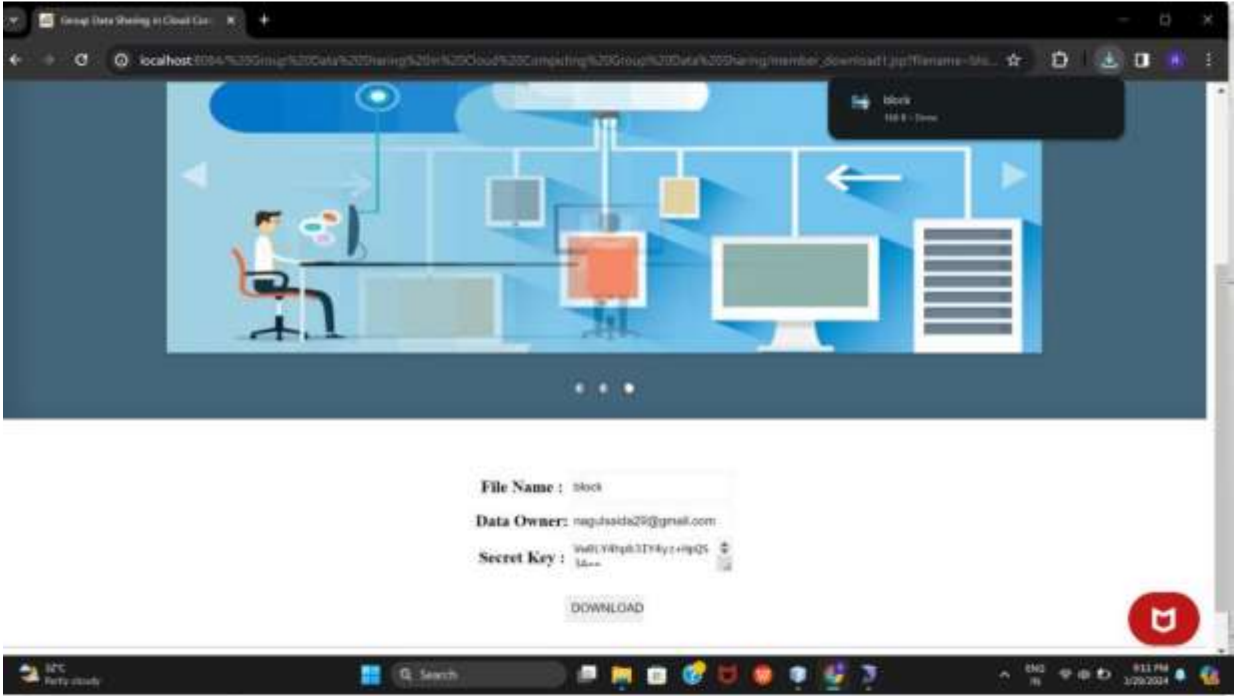
Key Sent



Verify Group Key

Group Name : mic

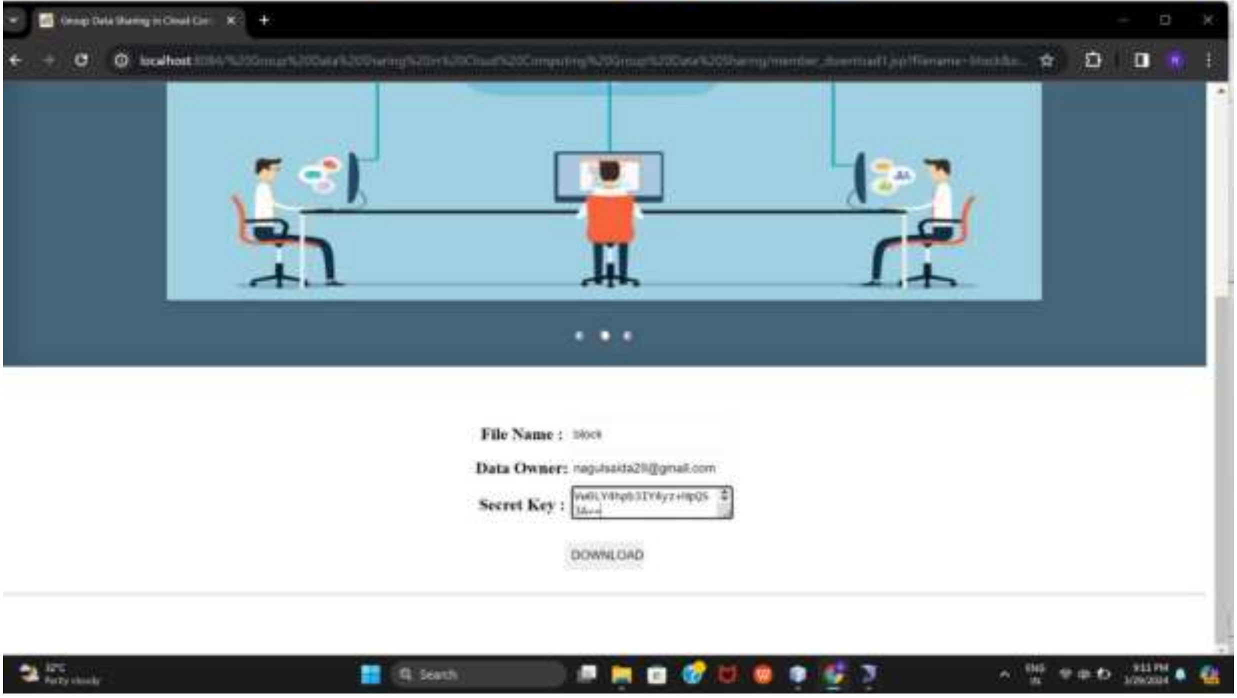
Group Key :



File Name : block

Data Owner: nagulsaida29@gmail.com

Secret Key : Vw8LY4hpb3TY4yz+i8pQS 34==



File Name : block

Data Owner: nagulsaida29@gmail.com

Secret Key : Vw8LY4hpb3TY4yz+i8pQS 34==

5.CONCLUSION

As an improvement inside the innovation of the net and cryptography, bunch data partaking in distributed computing has unfurled a fresh out of the box new space of value to pc organizations. With the help of the meeting key arrangement convention, the wellbeing and strength of bunch data partaking in distributed computing are frequently significantly moved along. In particular, the rethought information of the data property holders scrambled by the normal meeting key are safeguarded against the assaults of foes. Contrasted and gathering key appropriation, the meeting key arrangement has characteristics of higher wellbeing and unwavering quality. In any case, the gathering key understanding requests a lot of information communication inside the framework and a ton of system cost. To battle the issues inside the meeting key arrangement, the SBIBD is utilized inside the convention plan. during this paper, we tend to gift a novel block configuration based key understanding convention that supports bunch data partaking in distributed computing. in light of the definition and thusly the numerical depictions of the construction of a (v, k + 1, 1) plan, different members are many times worried inside the convention and general recipes of the normal meeting key for member are determined. Besides, the presentation of workers allows the gave convention to help the adaptation to internal failure property, in this way making the convention a ton of reasonable and secure. In our future work, we could like to stretch out our convention to deliver a ton of properties (e.g., obscurity, discernibility, so on) to shape it.

REFERENCES

[1] Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, and Yang Xiang, "Block Design-based Key Agreement for Group Data Sharing in Cloud Computing," IEEE Systems Journal, 2017.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," in IEEE INFOCOM, 2014, pp. 673–681.

[3] D. He, S. Zeadally, and L. Wu, "Certificate less public auditing scheme for cloud-assisted wireless body area networks," IEEE Systems Journal, pp. 1–10, 2015.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[5] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, "An efficient rfid authentication protocol providing strong privacy and security," Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016. [6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement," Designs Codes and Cryptography, vol. 28, no. 2, pp. 119–134, 2010.

[7] X. Yi, "Identity-based fault-tolerant conference key agreement," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 170–178, 2004.

[8] R. Barua, R. Dutta, and P. Sarkar, "Extending joux's protocol to multi party key agreement (extended abstract)." Lecture Notes in Computer Science, vol. 2003, pp. 205–217, 2003.

[9] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," Journal of Communications and Networks, vol. 14, no. 6, pp. 682–691, 2012.

[10] B. Dan and M. Franklin, "Identity-based encryption from the wail pairing," Siam Journal on C.

Author's Profiles:

#1:-Mrs.S.LAVANYA working as Assistant Professor in Department of IT in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

#2:-SK.RIZWANA(20H71A1230) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

#3:- Y.PRABHAS(20H71A1224) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

#4:- M.SHYAM(20H71A1239) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla521180

#5:- CH.SRINADH(21H75A1206) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180