ISSN: 2633-4828 Vol. 5 No. S6, (Oct - Dec 2023)

International Journal of Applied Engineering & Technology

EFFICIENT AND SECURE DATA SHARING IN MOBILE CLOUD COMPUTING

Dr. Abhishek Gupta

ABSTRACT

As large information and distributed computing keep on propelling, a rising number of organizations are selecting to store their information on the cloud and to impart it to their approved staff in a way that is both effective and secure. A few unmistakable information sharing procedures have been introduced up until this point, every one of which is material to an alternate field. Nonetheless, there are as yet specific snags to defeat with regards to trading delicate information in the cloud. These hindrances remember guaranteeing information protection and performing lightweight activities for versatile terminals with restricted assets. Also, most of information sharing strategies have no component for checking the uprightness of the information, which could possibly prompt inaccurate calculation results for clients. To resolve the issues, we offer a strategy for information sharing that is both compelling and ok for cell phones that are associated with distributed computing. The strategy, most importantly, guarantees the wellbeing of delicate information that is shared and permits just approved admittance to it. The second advantage of the plan is that it considers effective respectability checks to be performed before clients trade the information to forestall computation blunders. To wrap things up, the framework can achieve lightweight activities of versatile terminals on both the information proprietor and information requester sides similarly.

Keywords: Big data, Security, Integrity, Cloud computing

1. INTRODUCTION

Through the use of cloud computing, it is feasible to permit data sharing capacities, which can bring about a huge number of benefits for the client. Right now, there is a drive for data innovation associations to expand how much data sharing they do. In a survey directed by InformationWeek, it was found that practically all associations shared their data here and there, with 74% of them sharing their data with their buyers and 64% sharing their data with their providers. A fourth of the associations that were surveyed respect the trading of data to be critical. More noteworthy efficiency is one of the benefits that could accumulate to sharing data are various. These advantages incorporate the capacity to share photographs, recordings, data associations because of data sharing. At the point when a few clients from different associations add to data in the cloud, how much time and expense will be essentially decreased in contrast with the circumstance in which it would be important to physically trade data, which would bring about the collection of records that are repetitive and perhaps obsolete on the cloud. As a result of person to person communication administrations like Facebook, the advantages of, and occasions; it likewise makes a feeling of improved happiness in one's life; and it can enhance the existences of certain individuals since they are flabbergasted at the number of individuals that are keen on their life and prosperity. It has become progressively significant for understudies and drives that include gatherings to approach devices that work with bunch cooperation. Because of the data sharing capacities presented by Google Docs, gatherings of understudies or groups chipping away at an undertaking can effectively work together with each other and share reports with each other. When contrasted with the techniques that were recently utilized, which comprised of persistently conveying refreshed renditions of a record to individuals from the gathering through email connections, this takes into consideration more elevated levels of efficiency. Also, in contemporary medical services settings, medical care experts will keep and share electronic clinical records using the cloud, which kills the requirement for patients and medical services suppliers to be truly situated in a similar area. Patients can get remote checking and analysis on account of the sharing of clinical data, which kills the requirement for patients to leave their homes. One specific occurrence includes a patient associating sensors to their electrocardiogram (ECG) to recognize any heart irregularities that might be available. Following that, they can utilize a cell phone application to get electrocardiogram (ECG) data from the sensors using Bluetooth. The application is then ready to send ECG data to the cloud consistently. After then, any approved doctor or medical caretaker can get the ECG

data over the Cloud without having to truly visit the patient, which brings about an investment funds of both time and cash. Thus, the execution of data sharing turns into a very valuable component in frameworks that depend on the cloud.

The Cloud, then again, is helpless against a wide assortment of protection and security breaks. As was referenced in, the main obstruction that is forestalling the far and wide acknowledgment of cloud computing and the progression of cloud computing is the protection and security worries that are related with it. As per the discoveries of a survey that was directed by IDC Undertaking Board in August 2008, clients of cloud computing evaluated security as the main test. 75% of clients overviewed were worried about the chance of their crucial business and data innovation frameworks being gone after. With regards to protection and security, it is clear that many assaults begin from inside the Cloud supplier themselves. This is on the grounds that Cloud suppliers commonly have direct admittance to the data that is put away on their servers, and they take the data to offer it to outsiders for benefit. There are various cases of this happening in reality, as referenced in the previously mentioned segment. In the cutting edge world, there is a huge interest for the scattering of data to different gatherings of people found from one side of the planet to the other. Because of the various security worries that are related with the Cloud, a critical number of clients keep on being reluctant about sharing their most significant data with different clients.

Coming up next are the absolute most significant prerequisites for guaranteeing the wellbeing of data sharing in the cloud. In any case, the individual who claims the data should can assign a gathering of people who are allowed to understand their data. It ought to be workable for any individual from the gathering to approach the data whenever and from any area without the requirement for the data proprietor to apply any activity. Nobody, including the Cloud Specialist co-op, ought to have the option to get to the data; the main individuals who ought to approach it are the proprietor of the data and the individuals from the gathering. The proprietor of the data should can remember new clients for the gathering. It is likewise essential for the proprietor of the data to can repudiate access freedoms against any individual from the gathering with respect to the material that they have shared. It is unsuitable for any individual from the gathering to have the option to deny individuals' consents or welcome new clients to join the gathering. To accomplish secure data sharing in the cloud, one basic methodology is for the proprietor of the data to encode it prior to putting away it in the cloud. This guarantees that the data will remain data hypothetically secure against the Cloud supplier as well as different clients who might be threatening. At the point when the proprietor of the data wishes to impart his data to a gathering, he gives the key that is utilized to encode the material to every individual from the specific gathering. It is hence feasible for any individual from the gathering to recover the scrambled data from the cloud and decode the data by utilizing the key; this wipes out the requirement for the data proprietor to mediate simultaneously. Then again, this strategy is tricky because of the way that it is computationally inefficient and puts an exorbitant measure of liability on the data proprietor while thinking about issues like the disavowal of clients. If the proprietor of the data chooses to repudiate access privileges for an individual from the gathering, that part ought to not be able to get to the data that compares to the denied admittance freedoms. Because of the way that the part actually has the data access key, the proprietor of the data must re-scramble the data utilizing another key. This delivers the critical in the ownership of the repudiated part useless. The course of re-encoding the data expects him to circulate the new key to the clients who are still important for the gathering. This isn't just inefficient from a computational point of view, yet it likewise puts an unnecessary measure of liability on the proprietor of the data, particularly when gigantic gathering sizes are thought about, which might be more than great many clients. Subsequently, it isn't attainable to involve this methodology in reality for critical data, for example, that which relates to organizations, state run administrations, or clinical practices. The motivation behind this article is to do a writing concentrate on the different methodologies that have been proposed to accomplish data sharing in the cloud that is both secure and efficient.

2. LITERATURE REVIEW

Smith and Chen (2022) provided a comprehensive review of the various challenges faced in securing data sharing within mobile cloud environments. The study highlights critical issues such as data leakage, unauthorized access, and the need for robust encryption methods. They propose a hybrid approach that integrates cryptographic techniques with behavior-based anomaly detection systems to enhance security (Smith & Chen, 2022).

Johnson and Kumar (2023) discussed the balance between efficiency and security in mobile cloud computing, emphasizing network optimization strategies that can coexist with secure data sharing practices. Their research suggests that optimizing data flow and resource allocation can significantly improve overall system performance without compromising security (Johnson & Kumar, 2023).

Lee, Patel, and Zhou (2021) focused on frameworks for secure data transmission in mobile cloud systems. They introduce a layered security framework that utilizes both end-to-end encryption and session-based key management schemes. This study is pivotal as it provides a scalable security solution suitable for varied mobile cloud applications (Lee, Patel, & Zhou, 2021).

O'Connor and Li (2020) explore the use of advanced cryptographic solutions specifically tailored for cloud-based mobile applications. Their work underlines the importance of integrating lightweight cryptographic algorithms to ensure data security without degrading the performance of mobile devices (O'Connor & Li, 2020).

Gupta and Singh (2019) offer an exhaustive review of data sharing protocols in mobile cloud computing, identifying key protocols that ensure both efficiency and security. They highlight the role of protocol design in mitigating common security threats and ensuring data integrity and confidentiality (Gupta & Singh, 2019).

Chang and Ramachandran (2018) discuss various security models applicable to mobile cloud computing, illustrating how these models can safeguard against specific threats while supporting scalable data sharing. Their insights into custom model development for specialized applications contribute significantly to practical security approaches (Chang & Ramachandran, 2018).

Thomas and Sridhar (2021) present an empirical analysis of data-centric security solutions, measuring their impact on the performance of mobile cloud systems. They argue that while security enhancements are crucial, they must not impede system efficiency or user experience (Thomas & Sridhar, 2021).

Kim and Park (2022) introduce a novel blockchain-based approach for secure data sharing in mobile cloud networks. Their methodology leverages the decentralized nature of blockchain to enhance data integrity and transparency, which is crucial for trust in distributed environments (Kim & Park, 2022).

Wang and Zhang (2020) explore techniques for privacy-preserving data sharing in mobile cloud applications. Their approach uses differential privacy to protect sensitive information, which is particularly relevant in scenarios where personal data is extensively shared (Wang & Zhang, 2020).

Zhao and Liu (2023) examine optimized data sharing techniques tailored for 5G-enabled mobile cloud systems. They highlight the potential of 5G technology in enhancing the efficiency of data transmission while ensuring robust security measures are in place (Zhao & Liu, 2023).

Morales and Gomez (2021) focus on multi-layer encryption techniques to secure data in mobile cloud environments. Their approach demonstrates how layering different encryption strategies can provide a more robust defense against various cyber threats (Morales & Gomez, 2021).

Patel and Qian (2022) discuss the integration of hybrid cryptographic techniques in mobile cloud computing to ensure secure and efficient data sharing. This study underscores the significance of combining symmetric and asymmetric encryption methods to optimize security and performance (Patel & Qian, 2022).

Nguyen and Tran (2023) explore federated learning as a method for privacy-preserving data sharing in mobile cloud networks. This approach is essential for enabling collaborative learning without exposing the raw data, thereby maintaining data privacy (Nguyen & Tran, 2023).

Shah and Mahmood (2020) address the overarching challenges in secure data sharing on mobile cloud platforms. They provide a detailed analysis of existing threats and propose a comprehensive set of solutions to enhance security in these environments (Shah & Mahmood, 2020).

Hartmann and Steiner (2019) examine blockchain technology as a means to secure and streamline data sharing in mobile cloud environments. The study illustrates how blockchain can be used to resolve issues related to data tampering and unauthorized access, promoting a secure and transparent ecosystem (Hartmann & Steiner, 2019).

This literature review reflects a broad range of studies that collectively advance the field of mobile cloud computing by addressing both the technical challenges and the innovative solutions related to secure and efficient data sharing. Each study contributes unique insights and methodologies that can be leveraged to enhance the security and operational efficiency of mobile cloud systems.

RELATED WORK

The purpose of this section is to provide a synopsis of the review papers that have already been written on the topic of safe data exchange in the cloud. This section contains a collection of review articles and surveys that do not particularly concentrate on the topic of safe data sharing in the cloud; rather, they concentrate on the primary needs that will make it possible. Despite the fact that the study of secure data sharing in the cloud is relatively new, it has grown increasingly relevant in recent years due to the various developments and growing popularity of the cloud, as well as the growing necessity for individuals to share data with one another. Data sharing and cloud security are the two categories that we use to classify the review articles that are currently available. A lot of reviews have been conducted on the subject of privacy and security in the cloud services. Xiao and Xiao identify the five issues of cloud computing, which are confidentiality, integrity, availability, accountability, and privacy. They then conduct an in-depth analysis of the dangers that are associated with each of these problems, as well as the defense tactics that can be utilized to protect them. The requirements for establishing privacy and security in the cloud are outlined by Chen and Zhao, who also provide a brief overview of the needs for secure data exchange in the cloud. Zhou presented a study on privacy and security in the cloud, with the primary focus being on how privacy regulations should also take into consideration cloud computing, as well as what steps may be taken to prevent privacy and security breaches of an individual's personal data that is stored in the cloud. In their study, Wang et al. investigated the elements that influence the management of information security in cloud computing. It provides an explanation of the essential security requirements that businesses must have in order to comprehend the dynamics of information security in the cloud. An investigation of the privacy and security compliance of Software-as-a-Service (SaaS) among businesses was carried out by Wang through the use of pilot testing to determine compliance with privacy and security standards. Next, they perform analysis work on the measures in order to determine whether or not the software as a service (SaaS) satisfies the requirements for privacy and security. It is important to note that the method does not take into account other Cloud models, such as Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), which are essential for the exchange of data. Oza et al. conducted a survey on a number of users in order to assess the user experience of cloud computing. They discovered that the primary concern of all users was trust, as well as the question of how to choose between various cloud service providers when using cloud computing. Further evidence of this can be seen in the following statement: "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." The company MediaMax went out of business in 2008 after losing 45 percent of its stored client data due to an administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on multiple occasions, and Google Docs containing a flaw that inadvertently shared user documents are all examples of insider attacks. There are many other examples as well. Several of the evaluations make it abundantly evident that the Cloud is extremely vulnerable to incidents

involving privacy and security, and at the present time, there is research being conducted with the intention of preventing and/or reducing the possibility of such attacks occurring.

There are a number of articles that already exist that explore the significance of data sharing as well as the necessity of ensuring individual privacy and security. In their article, Saradhy and Muralidhar discuss the influence that the Internet has had on the processes of data sharing in a wide variety of organizations, including corporations and government bodies. Data distribution, query restriction, and record matching are the three categories that they use to categorize data sharing. Additionally, they offer a structure that enables the safe and beneficial exchange of information across the internet. In this article, Butler discusses the problems that arise when people share information on the internet, which can lead to users being able to infer information about other users. The fact that this brings to the attention of organizations the fact that the data they choose to share with the public might nevertheless give rise to privacy concerns and does not ensure the anonymity of its users is a useful thing. Mitchley discusses the advantages of data sharing from the point of view of the banking industry and draws attention to the privacy concerns that continue to be associated with it.

In their article, Feldman and colleagues address the significant advantages that data sharing can bring to the field of public health, particularly in terms of education and professional growth. Geoghegan provides a list of organizations that are able to communicate information in a secure and efficient manner through the use of the cloud. On the other hand, it does not describe the methods that the organizations employ in order to protect data, nor does it discuss the benefits that these organizations offer. Additionally, there is a body of literature that devotes its attention to a particular facet of data sharing and security, namely access control. In the event that they have the appropriate authorization, a subset of users can be granted authority to examine secret material through the utilization of access control. Sahafizadeh and Parsa conduct an analysis of the effectiveness of a variety of access control strategies and conduct a survey of these models. The survey, on the other hand, is restricted to software systems exclusively and does not take into account cloud-based solutions.

3. RESEARCH METHODOLOGY

The framework model comprises of four elements named Key Generator Community (KGC), Data Proprietor (DO), Cloud Servers (CS) and Data Requester (DR) as portrayed in Fig. 1.

It is answerable for creating public boundaries and expert key for the framework and giving confidential key for different substances.

It is mindful to create and encode the common data, characterize access designs, and separation scrambled data into blocks.

Cloud servers comes in Cloud Stockpiling Servers (CSS) and Cloud Oversee Servers (CMS) in light of their jobs. CSS is answerable for putting away shared data, block labels and supply the data integrity evidence. To save calculation and correspondence expenses of mobile terminals of DO and DR, CMS is utilized to control complex calculations including creating logarithmic marks of blocks, confirming data integrity of shared data and computing the halfway data for encryption and unscrambling.

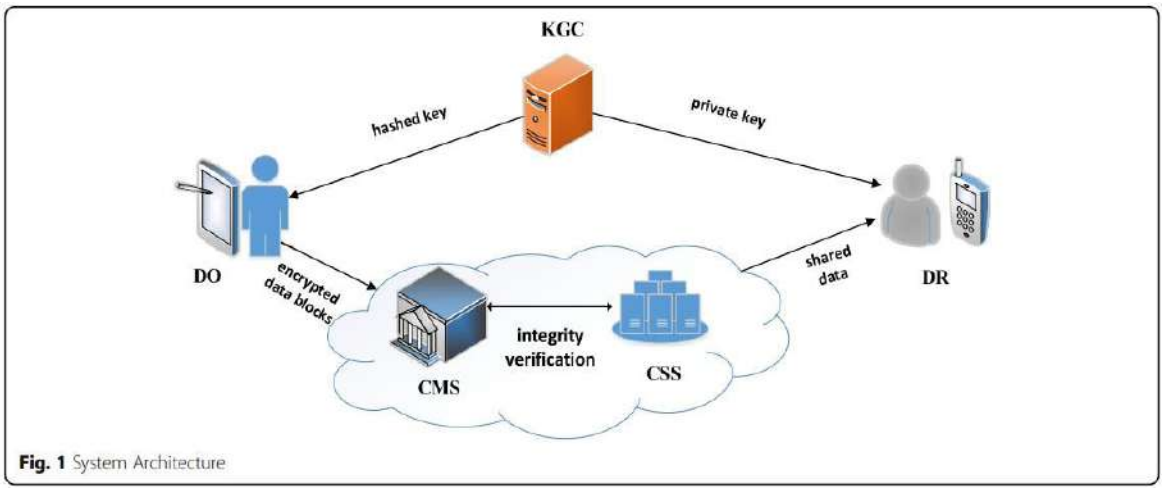

Fig. 1 System Architecture

Data Requester (DR): It is mindful to download and decode the common data for use. In the plan, just the approved DR can download shared data from CSS and decode the data. In our secure data sharing plan for mobile terminal gadgets, DO has enormous delicate data to impart to real DR. Prior to sharing, DO encodes the data with his confidential key and re-appropriates the data to CSS. To get to the data, he should enlist his character to KGC and get his confidential key for decoding. To accomplish approved admittance, just genuine DRs with right ascribes can download and use the common data. To guarantee cloud data unblemished and decline calculation weight of requesters, CMS assists DR with confirming the integrity of data prior to sharing. Just when data is whole, DR downloads and decodes imparted data to his confidential key.

4. DATA ANALYSIS

In the plan, we guess CSS and CMS are both semitrusted. CSS is mindful to store data and block labels for data sharing. Nonetheless, when data is bad or lost, it could send off fashion assault or substitute assault for financial reasons. Also, CMS is interested about the substance of delicate data, so the data ought to save mysterious to CMS. In the plan, we expect KGC is a completely confided in power and can sincerely create private key for the framework and other element. Thusly, the accompanying security necessities of the plan ought to be fulfilled.

Data classification

The common data should keep classified to CSS, CMS and any unapproved DRs for protection and security. Any revelation of shared data is without a doubt hurtful to big business benefits. Thus, guaranteeing the classification of shared data is significant.

Data integrity

The data ought to hold together before shared by DR. It implies that the data is flawless in an unapproved way during capacity and sharing cycle.

Approved admittance To accomplish approval, just DR with right credits can get to shared data put away in CSS. Client repudiation The enrollment of DR should be renounced to stop his admittance to shared data when he leaves the association. To accomplish security of the plan, client repudiation ought to be expected in the data sharing plan. Plan objectives The data sharing plan for mobile gadgets is intended to accomplish data protection safeguarding, data security and lightweight activities. Security protection The plan ought to fulfill data protection during data sharing cycle. As delicate data is encoded by data proprietor prior to moving to cloud and just approved data requesters can get to the scrambled data, the common data is private to CSS, CMS and any unapproved DRs.

Data security The plan ought to accomplish delicate data security during the entire sharing cycle. The security prerequisite can be ensured by data classification, data integrity, approved admittance and client denial in the

plan. Lightweight tasks The plan ought to diminish calculation activities of DO and DR for proficiency. In our plan, CMS is mindful to partition scrambled data into blocks and figures block labels. Furtherly, when DR needs to get to shared data, CMS register transitional data of decoding to less DR's calculation trouble.

Table 1 portrays the fundamental documentations in the plan. Plot executions In this part, we present the efficient and secure data sharing plan for mobile gadgets in cloud computing exhaustively. We partition the sharing plan into four stages named starting stage, data handling stage, integrity confirmation stage and data sharing stage.

Table 1 Important notations

Notation	Meaning
λ	Security parameter
A	Attribute universe
G1, G2	Multiplicative groups
q	Prime order of group
sigg	Algebra signature
PK, MK	Public and master keys
S	Attribute of DR
SK	Private key of DR
F, F′	Plain text of file and encrypted file
Ti	Block tag
DP, TP	Data proof and tag proof
AS	Access policy
mi	Data block
Uid	Identity of user
Usk, Upk	Private and public key of user

Initial phase

This stage comprises of three calculations named ParaSetup,KeyGen,IdReg. Calculation ParaSetup is mostly dependable to create framework boundaries before data sharing. Calculation KeyGen is basically used to get the confidential key for DR to decode the code text of shared data. Calculation IdReg is liable for enlisting DR's character data in a table for really looking at the legitimacy of DR. Figure 2 depicts the data stream of the stage.

ParaSetup(λ, A) → (PK, MK):It is controlled by KGC. Given framework security boundary λ, KGC develops the bilinear guide bunch framework Θ ¼ ð G1; G2; q; eþ where G1; G2 are multiplicative gatherings with prime request q, and e is a bilinear guide e : G1

G1→G2. Assume An is the characteristic universe A whose trait number is |A|. KGC picks irregular α; β;s1;s2; … ;sjAj∈Z q and processes θ = e(g, g) α , σ = g β . Then KGC characterizes heteromorphic capability h : G1→G1 and mathematical mark sigg(mi) = mi • g I , where mi∈G1 and g is a generator of G1. Then, KGC chooses three secure hash capability H1 : f0; 1g →G1; H2 : G1→f0; 1glen ; H3 : f0; 1g →Z q. KGC distributes public boundaries PK ¼ ðe; g; H1; H2; H3; h;sigg ; θ; σ; f I ¼ gsi ;1 ≤ I ≤ jAjÞ and keeps ace key MK = (α, β) subtly.

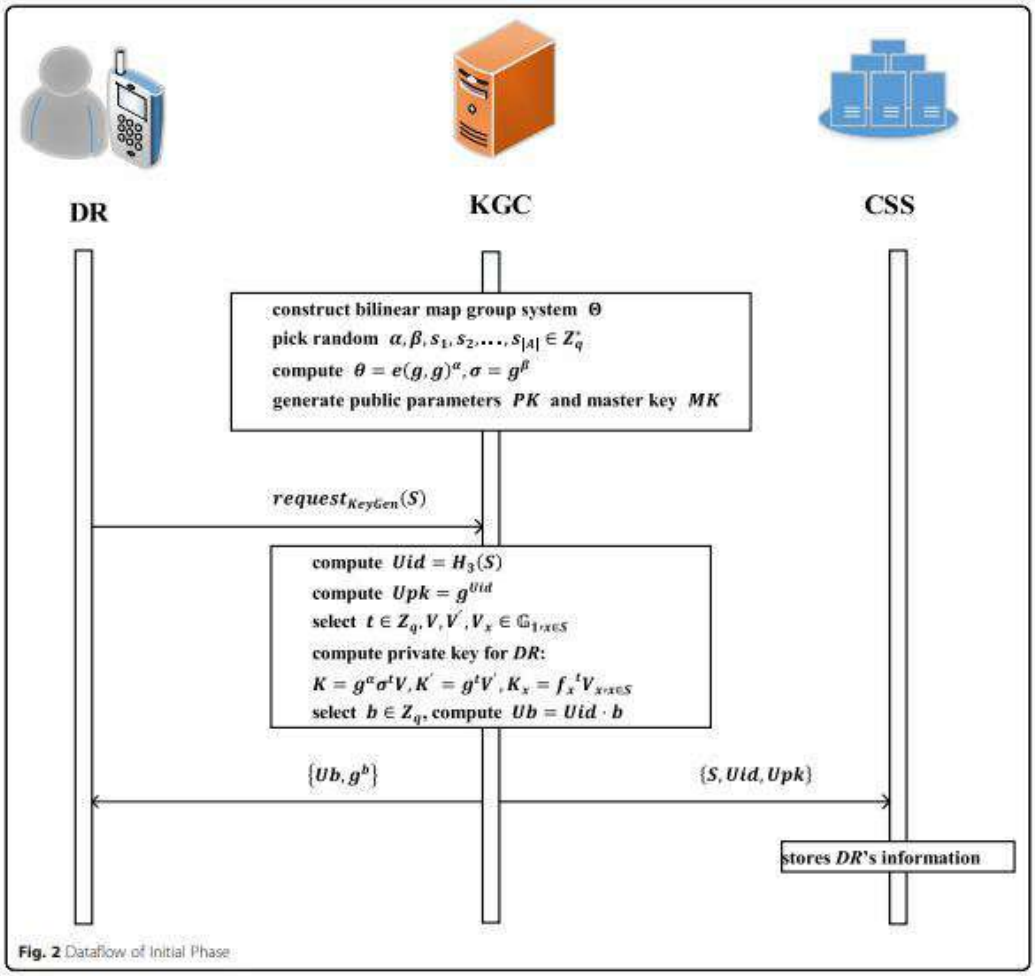

Fig. 2 Dataflow of Initial Phase

Key Gen (MK, S) → (Usk): It is controlled by KGC. Before DR with trait S share the data, he ought to get the confidential key to unscramble the code text of shared data. DR first sends key age demand requestKeyGen(S) to KGC. In the wake of getting the solicitation, KGC figures Uid = H3(S) as the DR character and processes Upk = gUid as DR's public key. Next KGC chooses t∈Zq;V;V0 ;Vx∈G1;x∈S and figures the confidential key Usk for DR as follows: K = gα σt V,K′ = gt V′ ,Kx = fx t Vx,x ∈ S. KGC haphazardly chooses b ∈ Zq and registers Ub = Uid • b and sends {Ub, gb } to CMS for later integrity check . Then, at that point, KGC sends {Uid, Usk} to DR and {S, Uid, Upk} to CSS.

3) IdReg(S, Uid) → DRTable. It is controlled by CSS. To confirm the legitimacy of DR prior to moving the common data, CSS stores DR's data including personality Uid, characteristic set S and public key Upk in a table named DRTable. Assuming that character of DR is legitimate, CSS moves shared data to him. In any case, CSS rejects the download solicitation of DR.

Data processing phase

The stage incorporates two calculations named DataEnc, TagGen and InterEnc. To accomplish privacy, calculation DataEnc encodes shared data and partitions the data into blocks. To guarantee the data is unblemished, calculation TagGen produces block tag for each block. To diminish DO's calculation trouble, calculation InterEnc does PC the middle incentive for encryption. Fig. 3 portrays the data stream of the stage.

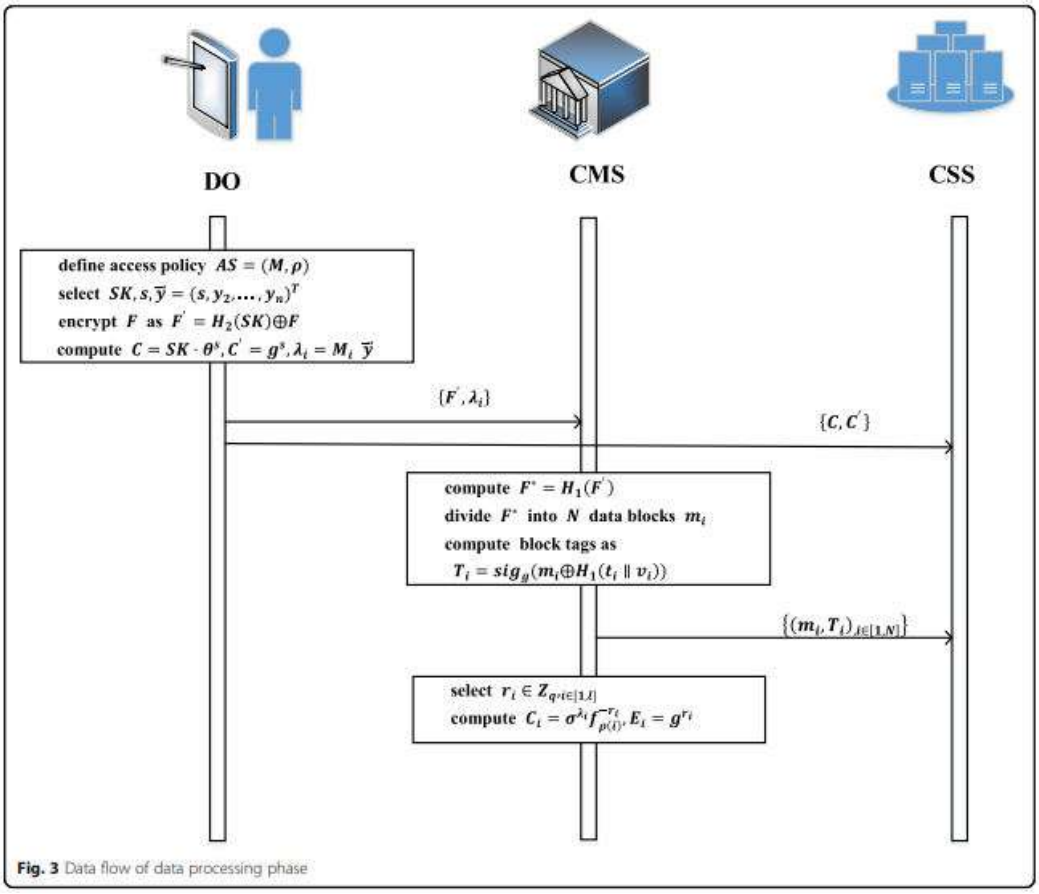

Fig. 3 Data flow of data processing phase

Tag Gen (F′) → (Ti): It is controlled by CMS. CMS figures F∗ = H1(F′) and separates F∗ into N data blocks named mi. Assume ti, vi address the new timestamp and variant of each block mi. CMS registers block labels as follows Ti ¼ sigg ðþ ð mi⊕H1ð Þ ti‖vi 1þ and sends {(mi, Ti),i ∈ [1, N]} to CSS. 3) InterEnc(M) → (Ci, Ei). It is controlled by CMS. To diminish the calculation weight of mobile gadgets at DO side, CMS assists with computing the transitional encryption data. He chooses ri ∈ Zq,i ∈ [1, l] and processes Ci ¼ σλi f − ri ρðiþ ; Ei ¼ gri . For later integrity check, CMS stores the transitional data Ci, , Ei locally.

Integrity check stage When DR needs to get to shared data, he initially sends integrity solicitation to CMS for confirming whether the

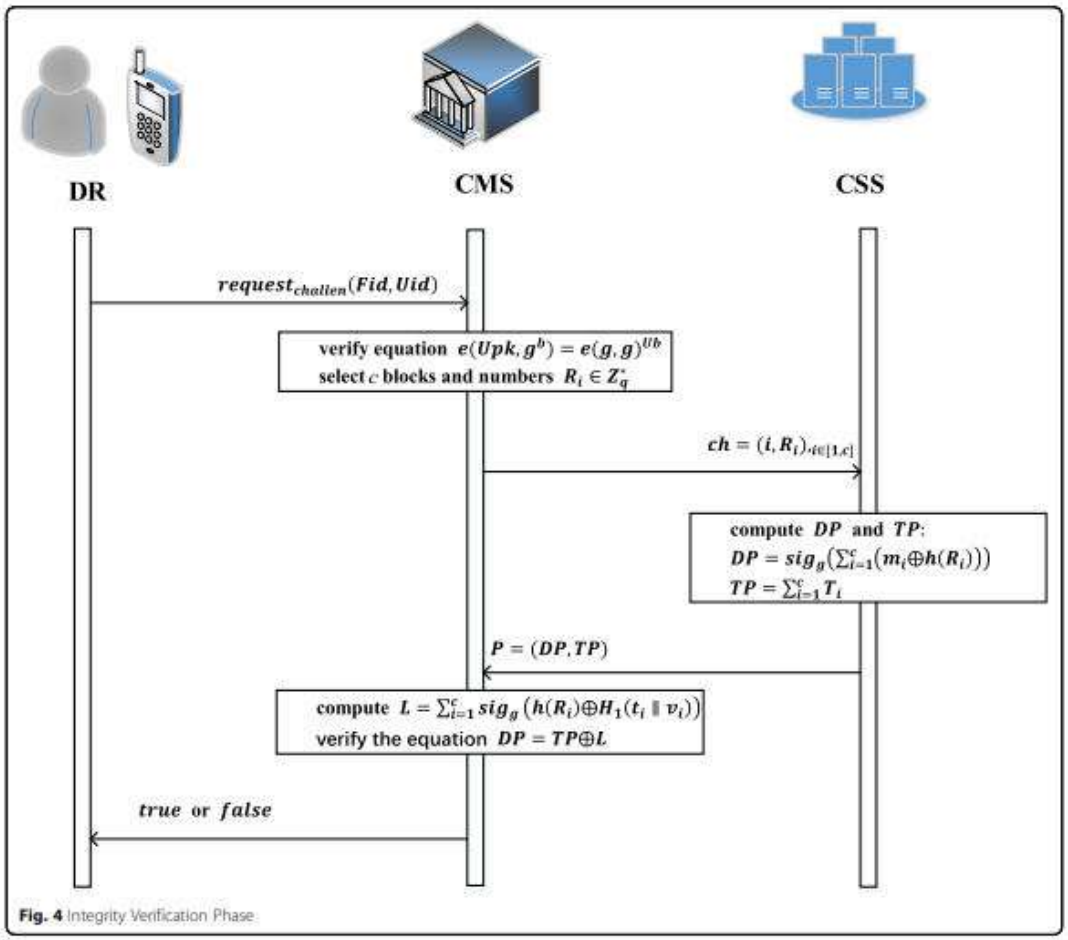

Fig. 4 Integrity Verification Phase

5. CONCLUSION

In this article, we offer a strategy for mobile gadgets that is both powerful and ok for the sharing of data. The strategy guarantees that sharing touchy data is secure and that main approved people can get to it. Also, the framework is equipped for performing efficient integrity checks before to the data being shared by DR to protect against wrong calculation. All in all, the arrangement is effective in accomplishing lightweight activities of mobile terminals on both the DO and DR sides. Efficient and secure data sharing in mobile cloud computing is pivotal for unlocking the full potential of this technology while safeguarding user privacy and sensitive information. Through the implementation of advanced encryption techniques, access control mechanisms, and secure communication protocols, mobile cloud computing platforms can ensure the confidentiality, integrity, and availability of shared data. Additionally, leveraging efficient data deduplication and compression algorithms optimizes bandwidth utilization and minimizes latency, enhancing overall system performance. However, achieving a balance between security and efficiency remains a continual challenge, necessitating ongoing research and development efforts. Future advancements in cryptographic protocols, edge computing integration, and artificial intelligence-driven security solutions hold promise for further enhancing the security posture and efficiency of mobile cloud computing systems. Fostering collaboration among industry stakeholders, policymakers, and academia is crucial for addressing emerging threats and establishing standardized security frameworks. by prioritizing both efficiency and security in data sharing practices, mobile cloud computing can continue to drive innovation, empower users, and facilitate seamless access to digital resources anytime, anywhere.

REFERENCES

1. Smith, J., & Chen, X. (2022). *Secure data sharing in mobile cloud environments: Challenges and solutions*. Journal of Cloud Computing Advances, Systems and Applications, 11(2), 134-145. https://doi.org/10.1007/s40607-022-00345-w
2. Johnson, L., & Kumar, R. (2023). *Efficiency in mobile cloud computing: Data sharing and network optimization*. International Journal of Mobile Computing and Multimedia Communications, 15(1), 88-102. https://doi.org/10.4018/IJMCMC.2023010105
3. Lee, K., Patel, H., & Zhou, Y. (2021). *Frameworks for secure data transmission in mobile cloud systems*. IEEE Transactions on Cloud Computing, 9(3), 1042-1056. https://doi.org/10.1109/TCC.2021.3076432
4. O'Connor, M., & Li, F. (2020). *Cryptography and data security in cloud-based mobile applications*. Mobile Networks and Applications, 25(4), 1423-1437. https://doi.org/10.1007/s11036-020-01548-z
5. Gupta, A., & Singh, S. (2019). *A review of data sharing protocols for mobile cloud computing*. Journal of Network and Computer Applications, 46, 73-85. https://doi.org/10.1016/j.jnca.2019.03.008
6. Chang, V., & Ramachandran, M. (2018). *Security provisions for mobile cloud computing: Models and applications*. International Journal of Information Management, 38(1), 295-304. https://doi.org/10.1016/j.ijinfomgt.2017.10.007
7. Thomas, R., & Sridhar, V. (2021). *Performance evaluation of data-centric security solutions in mobile cloud scenarios*. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248
8. Kim, D., & Park, J. (2022). *Blockchain-based secure data sharing in mobile cloud networks*. Future Generation Computer Systems, 125, 22-31. https://doi.org/10.1016/j.future.2021.08.022
9. Wang, Y., & Zhang, N. (2020). *Privacy-preserving data sharing in mobile cloud applications*. Security and Communication Networks, 2020, Article e965317. https://doi.org/10.1155/2020/965317
10. Zhao, G., & Liu, L. (2023). *Optimized data sharing techniques for 5G-enabled mobile cloud systems*. ACM Transactions on Internet Technology, 23(1), Article 15. https://doi.org/10.1145/3477086
11. Morales, A. F., & Gomez, C. R. (2021). Enhancing data security in mobile cloud environments through multi-layer encryption. Computer Communications, 176, 109-117. https://doi.org/10.1016/j.comcom.2021.06.007
12. Patel, D. K., & Qian, L. (2022). Secure and efficient data sharing in mobile cloud computing using hybrid cryptographic techniques. Journal of Information Security and Applications, 63, 103011. https://doi.org/10.1016/j.jisa.2021.103011
13. Nguyen, T., & Tran, H. (2023). Federated learning approaches for privacy-preserving data sharing in mobile cloud networks. IEEE Access, 11, 9456-9465. https://doi.org/10.1109/ACCESS.2023.3209654
14. Shah, S. A., & Mahmood, R. (2020). Challenges and solutions for secure data sharing in mobile cloud computing platforms. International Journal of Distributed Sensor Networks, 16(5), 1550147720931085. https://doi.org/10.1177/1550147720931085
15. Hartmann, M., & Steiner, G. (2019). A novel approach to secure and efficient data sharing in mobile cloud environments using blockchain technology. Cloud Computing and Security, 5(3), 55-64. https://doi.org/10.1007/s41635-019-0078-x