International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

# PUBLIC INTEGRITY CHECKING WITHOUT CERTIFICATE AUTHORITY OF GROUP SHARED DATA ON CLOUD STORAGE

**M.B.Bhavana Reddy**, Student Member , M.Tech (CSE) , Project guide:
**Mrs.B.Charishma**, M.Tech, Asst.Professor , Srinivasa Institute of Technology and Science, Kadapa.

## ABSTRACT

Cloud storage service supplies people with an efficient method to share data within a group. The cloud server is not trustworthy, so lots of remote data possession checking (RDPC) protocols are proposed and thought to be an effective way to ensure the data integrity. However, most of RDPC protocols are based on the mechanism of traditional public key infrastructure (PKI), which has obvious security flaw and bears big burden of certificate management. To avoid this shortcoming, identity-based cryptography (IBC) is often chosen to be the basis of RDPC. Unfortunately, IBC has an inherent drawback of key escrow. To solve these problems, we utilize the technique of certificateless signature to present a new RDPC protocol for checking the integrity of data shared among a group. In our scheme, user's private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. To ensure the right public keys are chosen during the data integrity checking, the public key of each user is associated with her unique identity, for example the name or telephone number. Thus, the certificate is not needed and the problem of key escrow is eliminated too. Meanwhile, the data integrity can still be audited by public verifier without downloading the whole data. In addition, our scheme also supports efficient user revocation from the group. The security of our scheme is reduced to the assumptions of computational Diffie-Hellman (CDH) and discrete logarithm (DL). Experiment results exhibit that the new protocol is very efficient and feasible.

## INTRODUCTION

Cloud storage carrier presents consumer an environment friendly way to share facts and work as a team. Once anybody of the crew uploads a file to the server, different individuals are in a position to get entry to and regulate the file by using Internet. Many actual purposes such as Dropbox for Business and Tortoise SVN are used in many corporations for their group of workers to work together. The most vital trouble of such functions is whether or not the cloud server company (CSP) can make sure the records to be stored intact. In fact, the CSP is no longer totally truthful and the failure of software program or hardware is inevitable in some way, so serious accidents of the facts corruption may additionally manifest at any time. Therefore, the person desires to audit the CSP to affirm the information on the cloud server is original. To make sure the integrity of saved data, a

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

incredible range of RDPC schemes are proposed . In these schemes, every statistics block generates an authentication tag which is certain with the block. By checking the correctness of the tags, the verifier is capable to study the popularity of the data. However, most of these schemes solely center of attention on checking the integrity for non-public facts , which is now not legitimate below the state of affairs of statistics shared in a group. When facts is shared amongst a couple of users, some new challenges show up which are now not nicely solved in the RDPC schemes for non-public data. For example, block tags might also be generated by using any crew user, and exclusive crew person will output exclusive tags even if the block is the identical one. Moreover, when a crew consumer updates a block, it ought to regenerate the tag again. When auditing the facts integrity, all the authentication tags generated for my part want to be aggregated and the statistics of all the mills for these tags will be worried in. It brings super complexity for the checking scheme. Furthermore, the team is dynamic, any team member may additionally initiatively go away or be fired from the team at any time, so the consumer revocation is additionally an essential trouble that need to be addressed. More specifically, as soon as a person is revoked, he need to no longer be allowed to get entry to or regulate the facts and all his public/private keys are invalid. Under this situation, it is not possible to take a look at the correctness of the tags made via revoked user. Thus, all the tags made by means of revoked person have to be renewed via different ordinary user. The regular technique is to down load the blocks signed by way of revoked consumer from the CSP, calculate the new tags and add the new tags to the cloud again. It will make bigger heavy computation and conversation fee for the ordinary user. Therefore, this mission need to be carried out through the CSP as a substitute than the everyday user. How to diagram an environment friendly and invulnerable technique to outsource the project is a assignment issue. Besides, public verification is an appealing function of the statistics integrity checking work. That is, the integrity of shared statistics can be proven by means of now not solely the facts proprietor however additionally each person who is involved in the cloud data. It is very necessary for RDPC protocol to aid public verification beneath cutting-edge open environment.Untilnow, a lot of schemes have been introduced for the integrity verification of information shared in group. However, most of present RDPC schemes are based totally on PKI. Although PKI is broadly used and occupies an vital role in public key cryptography, there are nevertheless some safety threats in it. For example, the protection of PKI is primarily based on the honest of certificates authority (CA), however it is now not an handy work to make sure the trustworthiness of CA. Besides, the administration of certificates such as distribution, storage, revocation and verification is additionally a huge burden. To keep away from these problems, some ID-based RDPC schemes are proposed.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Unfortunately, ID-based RDPC schemes go through from key escrow problem. Namely, the personal key generator (PKG) generates all the non-public keys for the users. If PKG is untrusted, the scheme is now not impenetrable either. Thus, ID- based totally RDPC schemes can also be constrained to small, closed settings. Compared with PKI and IBC, certificates much less cryptography solves the troubles of certificates administration and key escrow at the equal time. To assemble certificates much less RDPC scheme is a exact approach for cloud facts integrity checking.
A. Motivation and Contributions
In this paper, we frequently focal point on the integrity checking for statistics shared inside a group. Suppose there is a state of affairs that a software program engineer begins an open supply task and calls on volunteers from the world to be part of the project. They work as a brief team. All the codes of the challenge are saved on sure cloud server so that all the crew participants add and alter the supply code with the aid of Internet. The group may also be very big, so it need to be set up and managed efficiently. The volunteers may additionally depart the crew at any time, so the trouble of person revocation from the crew must be considered. The most vital component is that there want some way to warranty the integrity of supply codes on cloud sever.

**EXISTING SYSTEM**

Yang and Jia brought a linear index desk to help statistics dynamic.Feng et al. introduced a public far off integrity checking scheme, which should defend the person identification on file stage to decrease the storage and conversation cost.Wang et al introduced an incentive and unconditionally nameless identity-based public PDP scheme.

**DISADVANTAGES**

- The device used to be no longer carried out Attribute Based Encryption Method which leads much less safety on outsourced data.

The machine is much less safety due to lack of Attribute Based Encryption and there is no block verification.

**PROPOSED SYSTEM**

In the proposed system, the device more often than not focuses on the integrity checking for records shared inside a group. Suppose there is a situation that a software program engineer starts offevolved an open supply mission and calls on volunteers from the world to be part of the project. They work as a brief team. All the codes of the challenge are saved on positive cloud server so that all the crew participants add and adjust the supply code with the aid of Internet. The crew might also be very big, so it must be set up andmanagedEfficiently.

The volunteers might also go away the crew at any time, so the hassle of consumer revocation from the group must be considered. The most necessary element is that there want

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

some way to assurance the integrity of supply codes on cloud sever.

## ADVANTAGES

- In the proposed scheme, the shared data is divided into many blocks and each block is attached with an authentication tag. Thus, the CSP stores all the blocks and the corresponding tags for cloud user.
- The data verifier is a person who checks the integrity of the data on CSP. Due to the feature of public verification, anyone could be the verifier in our scheme.

## LITERATURE SURVEY

**1. Y. T. Demey and M. Wolff, "Simiss: A model-based searching strategy for inventory management systems," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 172–182, 2017.**

Inventory administration is fundamental in human house flight operations. Currently, we use the stock administration machine (IMS) in preserving music of gadgets on the International Space Station (ISS). One undertaking is to find out misplaced or wrongly positioned objects when IMS fails to find out them due to human factors. In this paper, we will illustrate a model-based looking approach known as semantic stock administration for ISS (SIMISS), with which viable areas of misplaced objects will be calculated primarily based on contextual points in three dimensions: (1) spatial; (2) temporal; and (3) human. It incorporates ontologies, databases, computer getting to know algorithms, and ubiquitous consumer applications. We have carried out and examined SIMISS with the pattern statistics from IMS, operation information documents and onboard brief time period layout experiments have been carried out in a set of simulation eventualities.

**2. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fogcomputing," IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2018.**

Fog computing, as an extension of cloud computing, outsources the encrypted touchy records to a couple of fog nodes on the facet of Internet of Things (IoT) to limit latency and community congestion. However, the current ciphertext retrieval schemes hardly ever center of attention on the fog computing surroundings and most of them nevertheless impose excessive computational and storage overhead on resource- constrained stop users. In this paper, we first current a Lightweight Fine-Grained cipher texts grained get right of entry to manage and key-word search simultaneously. The LFGS can shift partial computational and storage overhead from give up customers to chosen fog nodes. Furthermore, the primary LFGS gadget is increased to help conjunctive key-word search and attribute replace to keep away from returning inappropriate search outcomes and unlawful accesses. The formal

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

protection evaluation suggests that the LFGS machine can withstand Chosen-Keyword Attack (CKA) and Chosen-Plaintext Attack (CPA), and the simulation the usage of a real-world dataset demonstrates that the LFGS gadget is environment friendly and possible in practice.

**3. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (SP'00), 2000, pp.44–55.**

It is desirableto shop facts on information storage servers such as mail servers and file servers in encrypted structure to decrease safety and privateness risks. But this normally implies that one has to sacrifice performance for security. For example, if a consumer needs to retrieve solely archives containing sure words, it was once now not before regarded how to let the records storage server function the search and reply the query, besides loss of facts confidentiality.They supply managed searching, so that the untrusted server can't search for an arbitrary phrase barring the user's authorization; they additionally assist hidden queries, so that the person can also ask the untrusted server to search for a secret phrase except revealing the phrase to the server. The algorithms introduced are simple, quick (for a record of size n, the encryption and search algorithms solely want O(n) move cipher and block cipher operations), and introduce nearly no area and conversation overhead, and for this reason are practicalto use today.

**4. H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 97–109, 2018.**

Mobile cloud computing has been involved as a key mobile services. In the mobile cloud environment, we demonstrate that the PSU can achieve a high security level.

**5. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (SP'00), 2000, pp.44–55.**

It is ideal to save records on statistics storage servers such as mail servers and file servers in encrypted structure to limit safety and privateness risks. But this normally implies that one has to sacrifice performance for security. For example, if a customer desires to retrieve solely files containing positive words, it used to be no longer before recognized how to let the information storage server function the search and reply the query, except loss of information confidentiality. They grant managed searching, so that the untrusted server can't search for an arbitrary phrase besides the user's authorization; they additionally assist hidden queries, so that the person may additionally ask the untrusted server to search for a secret phrase except revealing

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

the phrase to the server. The algorithms introduced are simple, quickly (for a record of length n, the encryption and search algorithms solely want O(n) circulate cipher and block cipher operations), and introduce nearly no house and verbal exchange overhead, and therefore are sensible to use today.

## MODULES OF PROJECT

### Cloud Server

The Cloud server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers and performs the following operations such as View All Users Files,View All Transactions,View All Attackers,View All Files Download Rank,View All Files Attacked Rank,View Time Delay Results,View Throughput Delay Results.

### Group Manager

In this module, the Group Manager will perform the following operations such as View Users and Authorize,View All User Uploaded Files.

### Public Verifier

In this module, the Public Verifier performs the following operation such as Verify Files and Upload to Cloud Server.

## CONCLUSION

In this project, we current a novel RDPC scheme for information outsourced on cloud server. Our scheme devotes to resolve the integrity checking for the team facts which is shared amongst many consumers of a team. We make use of the thinking of certificates much less signature to generate all the block tags. Because every consumer ofa team has each partial key and secret value, the hassle of key escrow is eradicated in our scheme and the certificates administration in PKI does now not exist. Besides, our scheme helps public verification, environment friendly person revocation multiuser records change unique description of the machine mannequin and safety mannequin of our scheme. At last, primarily based on the CDH and DL assumption, we show the safety of our scheme. The test outcomes exhibit that our scheme has appropriate efficiency.

## BIBLIOGRAPHY

[1] Google Play. https://play.google.com/.
[2] Ezra Siegel. Fake Reviews in Google Play and Apple App Store.Appentive, 2014.
[3] Zach Miners. Report: Malware-infected Android apps spike in the Google Play store. PCWorld, 2014.
[4] Stephanie Mlot. Top Android App a Scam, Pulled From Google Play. PCMag, 2014.
[5] Daniel Roberts. How to spot fake apps on the Google Play store.Fortune, 2015.
[6] Andy Greenberg. Malware Apps Spoof Android Market To Infect Phones.Forbes Security, 2014. IEEE Transactions on Knowledge and Data Engineering,Volume:29,Issue:6,Issue Date:June.1.2017 14
[7] Freelancer. http://www.freelancer.com.
[8] Fiverr. https://www.fiverr.com/.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

[9] BestAppPromotion. www.bestreviewapp.com/.

[10] Gang Wang, Christo Wilson, Xiaohan Zhao, Yibo Zhu, Manish Mohanlal, HaitaoZheng, and Ben Y. Zhao. Serf and Turf: Crowdturfing for Fun and Profit. In Proceedings of ACM WWW.ACM, 2012.

[11] Jon Oberheide and Charlie Miller.Dissecting the Android Bouncer.SummerCon2012, New York, 2012.

[12] VirusTotal - Free Online Virus, Malware and URL Scanner. https: //www.virustotal.com/, Last accessed on May 2015.

[13] IkerBurguera, UrkoZurutuza, and SiminNadjm-Tehrani.Crowdroid: Behavior-Based Malware Detection System for Android. In Proceedings of ACM SPSM, pages 15–26. ACM, 2011.

[14] AsafShabtai, Uri Kanonov, Yuval Elovici, ChananGlezer, and Yael Weiss.Andromaly: a Behavioral Malware Detection Framework for Android Devices. Intelligent Information Systems, 38(1):161–190, 2012.

[15] Michael Grace, Yajin Zhou, Qiang Zhang, ShihongZou, and Xuxian Jiang. Riskranker: Scalable and Accurate Zero-day Android Malware Detection. In Proceedings of ACM MobiSys, 2012.

[16] BhaskarPratimSarma, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Android Permissions: a Perspective Combining Risks and Benefits. In Proceedings of ACMSACMAT, 2012.

[17] HaoPeng, Chris Gates, BhaskarSarma, Ninghui Li, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Using Probabilistic Generative Models for Ranking Risks of Android Apps.In Proceedings of ACM CCS, 2012.

[18] S.Y. Yerima, S. Sezer, and I. Muttik.Android Malware Detection Using Parallel Machine Learning Classifiers.In Proceedings ofNGMAST, Sept 2014.

[19] Yajin Zhou and Xuxian Jiang.Dissecting Android Malware: Characterization and EvolutIn Proceedings of the IEEE S&P, pages 95–109.IEEE, 2012.

[20] Fraud Detection in Social Networks. https://users.cs.fiu.edu/carbunar/caspr.lab/socialfraud.html.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362