IJPREMS

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 354-358

e-ISSN : 2583-1062

Impact Factor : 5.725

A LIGHTWEIGHT AND PRIVACY DATA DYNAMICS IN CLOUD COMPUTING

Sureshkumar T[1], Agalya C[2], Harshini K S[3], Nivashini K S[4], Poojitha S[5]

[1]Assistant Professor, Department of Information Technology, Nandha College of Technology, Perundurai 638 052, Tamil Nadu, India.

[2,3,4,5]UG Students - Final Year, Department of Information Technology, Nandha College of Technology, Perundurai 638 052, Tamil Nadu, India.

ABSTRACT

Cloud Computing is made out of various circulated Cloud Computing, which are framed on-the-fly by powerfully incorporating underutilized Cloud Computing assets including figuring force, stockpiling, etc. The diversity of devices used to access the services and data. Thus in this paper, we present a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among geographically dispersed physical devices and clients. The proposed protocol is demonstrated to resist chosen-cipher-text attack (CCA) under the hardness assumption of decisional-Strong Diffie-Hellman (SDH) problem. We also evaluate the performance of the proposed protocol with existing data sharing protocols in terms of computational overhead, communication overhead, and response time. We initially propose an improved cipher-text-strategy characteristic based encryption (CPABE) plot**.**

Keywords – Encryption, Decryption, Private Storage, Diffie Hellman Key Exchange, Public and Private Key, Cloud Storage.

1. INTRODUCTION

Vehicular conveyed figuring (VCC), the coordination of the headways of dispersed processing and vehicular associations , is gaining thought in light of its capacities of supporting a movement of novel, significant, and moreover tricky applications for working on driving security, saving energy, overhauling the traffic, and so forth . Like dispersed processing giving cloud organizations, VCC can give distinctive compact vehicular cloud organizations for vehicles. Exactly when a vehicle needs to get to VCC organizations, VCC expert communities (VCCSP) regularly require the vehicle's conspicuous information to support its requesting.

1.1 Cloud Computing

Circulated registering is the on-demand availability of PC structure resources, especially data accumulating (dispersed capacity) and figuring power, without direct unique organization by the customer. The term is all around used to depict server ranches open to various customers over the Internet. Gigantic fogs, overpowering today, as often as possible have limits passed on over various regions from central laborers. If the relationship with the customer is decently close, it may be allotted an edge specialist. Fogs may be limited to a singular affiliation (attempt fogs), or be open to various affiliations (public cloud). Circulated registering relies upon sharing of resources for achieve coherence and economies of scale. Backers of public and crossbreed fogs note that circulated figuring grants associations to avoid or restrict ahead of time IT structure costs. Advocates also ensure that circulated processing grants dares to prepare their applications for activity speedier, with further developed reasonableness and less help, and that it engages IT gatherings to even more rapidly change resources for fulfill fluctuating and surprising need, giving the burst enlisting capacity: high figuring power at explicit occasions of apex interest. Cloud providers normally use a "pay-all the more just as expenses emerge" model, which can incite unanticipated working expenses assuming chiefs are not familiar with cloud-assessing models. The openness of high-limit associations, ease PCs and limit contraptions similarly as the certain gathering of hardware virtualization, organization organized plan and autonomic and utility handling has provoked improvement in circulated figuring. Distributed computing is an organization access model that intends to straightforwardly and pervasively share an enormous number of registering assets. These are rented by a specialist organization to advanced clients, generally through the Internet. Because of the expanding number of auto collisions and disappointment of street clients in vehicular organizations, the significant focal point of current arrangements given by canny transportation frameworks is on further developing street wellbeing and guaranteeing traveler solace. Distributed computing innovations can possibly further develop street wellbeing and voyaging experience in ITSs by giving adaptable arrangements (i.e., elective courses, synchronization of traffic signals, and so on) required by different street security entertainers like police, and fiasco and crisis administrations. To further develop traffic wellbeing and offer computational types of assistance to street clients, another distributed computing model called VANET-Cloud applied to vehicular specially appointed organizations is proposed. Different transportation administrations given by VANET-Cloud are audited, and some future examination headings are featured, including security and protection, information conglomeration, energy effectiveness, interoperability, and asset the executives.

1.2 Motivation

VANETs will have exceptional necessities of independent vehicles with high versatility, low dormancy, ongoing applications, and network, which may not be settled by ordinary distributed computing. Henceforth, converging of mist processing with the regular cloud for VANETs is talked about as a likely answer for quite some time in current and future VANETs. What's more, mist registering can be upgraded by incorporating Software-Defined Network (SDN), which gives adaptability, programmability, and worldwide information on the organization.

1.3 Summary

With millions of users around the world, real time search systems and different types of mining tools are emerging to allow people tracking the impact of events and news on social network sites. Detecting spammers in social network sites plays an important role. The overall outline of the current work has given in this chapter. The works related to the spam detection is given in the next Chapter 2, Review of Literature.

2. RELATED WORKS

2.1 Lightweight Delegatable Proofs of Storage

J. Xu, A. Yang, J. Zhou, and D. S. Wong et.al says, Cloud storage has been in widespread use nowadays, which alleviates users’ burden of local data storage. Meanwhile, how to ensure the security and integrity of the outsourced data stored in a cloud storage server has also attracted enormous attention from researchers. Proofs of storage (POS) is the main technique introduced to address this problem. Publicly verifiable POS allowing a third party to verify the data integrity on behalf of the data owner significantly improves the scalability of cloud service. However, most of existing publicly verifiable POS schemes are extremely slow to compute authentication tags for all data blocks due to many expensive group exponentiation operations, even much slower than typical network uploading speed, and thus it becomes the bottleneck of the setup phase of the POS scheme. In this article, we propose a new variant formulation called “Delegatable Proofs of Storage (DPOS)”. Then, we construct a lightweight privacy-preserving DPOS scheme, which on one side is as efficient as private POS schemes, and on the other side can support third party auditor and can switch auditors at any time, close to the functionalities of publicly verifiable POS schemes. Compared to traditional publicly verifiable POS schemes, we speed up the tag generation process by at least several hundred times, without sacrificing efficiency in any other aspect. LOUD computing has been widely accepted and deployed in our daily life due to the great benefits that it brings about such as decreasing infrastructure costs, providing high scalability and availability. More and more people rely on cloud storage services to reduce their local storage burden. Namely, data is outsourced to the cloud server and can be accessed on demand later. Meanwhile, how to ensure the security and integrity of the outsourced data without keeping a local copy for data owners is an imperative concern to address. One of the main solutions is to apply proofs of storage (POS) that is also referred to proofs of retrievability (POR) or proofs of data possession (PDP) , in which the integrity of data stored in cloud server can be verified without having to download all the data. The basic idea is dividing the whole data file into multiple blocks, each of which is used to generate a homomorphic verifiable tag (HVT) sent to the cloud server together with the data file. Since the first POR and PDP schemes are presented in 2007, there have been lots of efforts devoted to constructing proofs of storage schemes with more advanced features such as public key verifiability , data dynamics, (i.e. modifying/inserting/deleting data blocks), multiple cloud servers and data sharing .

2.2 PORS: Proofs of Retrievability for Large Files

Cloud storage has been in widespread use nowadays, which alleviates users' burden of local data storage. Meanwhile, how to ensure the security and integrity of the outsourced data stored in a cloud storage server has also attracted enormous attention from researchers. Proofs of storage (POS) is the main technique introduced to address this problem. Publicly verifiable POS allowing a third party to verify the data integrity on behalf of the data owner significantly improves the scalability of cloud service. However, most of existing publicly verifiable POS schemes are extremely slow to compute authentication tags for all data blocks due to many expensive group exponentiation operations, even much slower than typical network uploading speed, and thus it becomes the bottleneck of the setup phase of the POS scheme. In this article, we propose a new variant formulation called “Delegatable Proofs of Storage (DPOS)”. Then, we construct a lightweight privacy-preserving DPOS scheme, which on one side is as efficient as private POS schemes, and on the other side can support third party auditor and can switch auditors at any time, close to the functionalities of publicly verifiable POS schemes. Compared to traditional publicly verifiable POS schemes, we speed up the tag generation process by at least several hundred times, without sacrificing efficiency in any other aspect. In addition, we extend our scheme to support fully dynamic operations with high efficiency, reducing the computation of any data update to O(log n) and simultaneously only requiring constant communication costs. We prove that our scheme is sound and privacy preserving against auditor in the standard model. Experimental results verify the efficient performance of our scheme.

2.3 Hybrid Provable Data Possession at Untrusted Stores in Cloud Computing

G. Ateniese, R. Burns, R. Curtmola, et.al has proposed In recent years, cloud computing has gradually become the mainstream of Internet services. When cloud computing environments become more perfect, the business and user will be an enormous amount of data stored in the remote cloud storage devices, hoping to achieve random access, data collection, reduce costs, and facilitate the sharing of other services. However, when the data is stored in the cloud storage device, a long time, enterprises and users inevitably will have security concerns, fearing that the information is actually stored in the cloud is still in the storage device or too long without access to, has long been the cloud server removed or destroyed, resulting in businesses and users in the future can't access or restore the data files. Therefore, this scheme goal to research and design for data storage cloud computing environments that are proved. Stored in the cloud for data storage, research and develop a security and efficient storage of proof protocol, also can delegate or authorize others to public verifiability whether the data actually stored in the cloud storage devices.

2.4 Dynamic Provable Data Possession

C. Erway, A. Kupc¸ u, C. Papamanthou, et.al has proposed in cloud storage scenarios, data security has received considerably more attention than before. To ensure the reliability and availability of outsourced data and improve disaster resilience and data recovery ability, important data files possessed by users must be stored on multiple cloud service providers (CSPs). However, we know that CSP is invariably not reliable. In this situation, to verify the integrity of replica files stored by users on multiple CSPs simultaneously, a new dynamic multiple-replica provable data possession (DMR-PDP) scheme is proposed. In addition, due to the importance of the tag set, we utilize vector dot products instead of using the modular power calculation in the traditional PDP scheme, which greatly reduces the calculation time and storage space usage. Moreover, a novel dynamic data structure, the divided address version mapping table (DAVMT), is presented and used to solve the problem of data dynamic operation.

2.5 MR-PDP: Multiple-Replica Provable Data Possession

R. Curtmola, O. Khan, R. Burns, et.al has proposed Many storage systems rely on replication to increase the availability and durability of data on untrusted storage systems. At present, such storage systems provide no strong evidence that multiple copies of the data are actually stored. Storage servers can collude to make it look like they are storing many copies of the data, whereas in reality they only store a single copy. We address this shortcoming through multiple-replica provable data possession (MR-PDP): A provably-secure scheme that allows a client that stores t replicas of a file in a storage system to verify through a challenge-response protocol that (1) each unique replica can be produced at the time of the challenge and that (2) the storage system uses t times the storage required to store a single replica. MR-PDP extends previous work on data possession proofs for a single copy of a file in a client/server storage system (Ateniese et al., 2007). Using MR-PDP to store t replicas is computationally much more efficient than using a single-replica PDP scheme to store t separate, unrelated files (e.g., by encrypting each file separately prior to storing it). Another advantage of MR-PDP is that it can generate further replicas on demand, at little expense, when some of the existing replicas fail.

3. PROPOSED METHODOLOGY

Identity-Based Online/Offline Digital Signature (CP-ABE with Diffe Hellman) is the proposed algorithm that is used. In order to increase the performance of WSNs we use an efficient and constructive method called clustering. The survey is concerned with the secure data transmission for Cluster-based Wireless Sensor Networks (CWSN). To achieve energy competence we have introduced two new Secure and Efficient Data Transmission (SET) protocols. CP-ABE with Diffe Hellman which is based on the Identity-Based Digital Signature (IBS) scheme and Identity-Based Online/Offline Digital Signature (CP-ABE with Diffe Hellman) scheme which makes improvement to the existing lightweight CP-ABE scheme deffie hell-man algorithm in order to make it more efficient architecture , by adopting the improved CP-ABE. To realize secure access user, the information is encrypted by the improved proposed method and uploaded to the VC in the form of cipher text. Firstly, the participation of trusted authority is reduced, which can decrease communication overhead on both trusted authority and each VC. There is a central controller which contains the detail of content server, RSU **(ROAD SIDE UNIT)** details and the vehicle details. As many number of control server can be generated with the rsu and the available content server id will be shown in the respected rsuform. The rsu can be connected to the content server as the user required and the vehicle node details will be shown in the rsu form. Data replication can be done in the vehicle as the nearest rsu is available.

3.1 Encryption Module

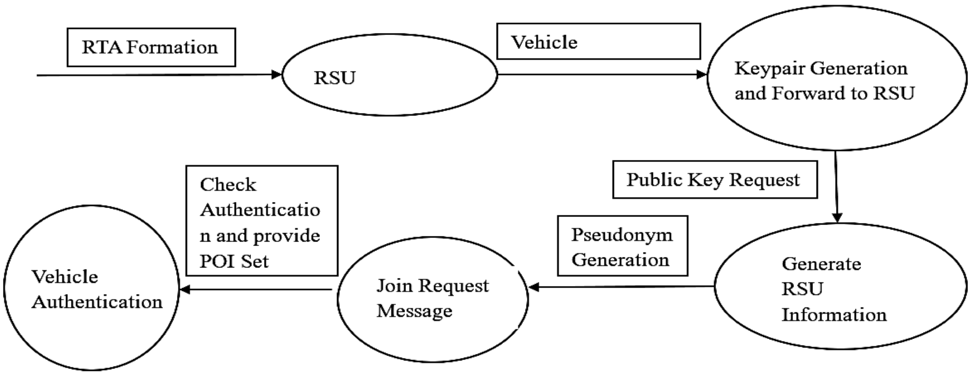
CP-ABE based IBOOS plan chooses a lot of characteristics to each customer. Every quality worth has a private key. The scramble or fosters a technique for unraveling. Customers whose attributes don't satisfy the technique can't unscramble the ciphertext. Proposed a lightweight CP-ABE plot for flexible cloud helped digital actual structures, which has three estimations as follows. This estimation is at risk for disseminating public limits and keeping a specialist secret key securely for the whole system. Encryption: This estimation is responsible for creating the ciphertext through contributing the public limits, data, and access procedure. By then the ciphertext is moved to the cloud. Unscrambling: This computation is at risk for recovering the data with the ciphertext, pro secret key, and a lot of characteristics.

3.2 Central Controller Server

In the focal regulator module the rsusubtleties, accessible substance server id, and the reaching the closest vehicle through rsu every one of the subtleties can be kept up with. This module holds as the focal center as the rsu goes under the substance server, rsu id and the area id can be seen and made in the server. Information replication in the vehicle likewise done in a piece of server. Programming characterized organizations can be automatically arranged, that is, network overseers can compose their own SDN projects to design, oversee, secure, and enhance network assets by means of robotized scripts. For this, open and vanet strategy are required, as we lay out. The advantage of open application programming interfaces (APIs) is that a server lock-in is kept away from. Through this deliberation, it doesn't make any difference which equipment is utilized, comparatively to PCs.

3.3 BI Linear Paring Module

The calculation of bilinear pairings has been viewed as the most costly activity in blending based cryptographic conventions. In this paper, we initially propose an effective and secure re-appropriating calculation for bilinear pairings in the two untrusted program model. Contrasted and the cutting edge calculation, a distinctive property of our proposed calculation is that the (asset obliged) outsourcer isn't needed to play out any costly tasks, for example, point augmentations or exponentiations. Besides, we use this calculation as a subroutine to accomplish reevaluate secure character based encryptions and marks.

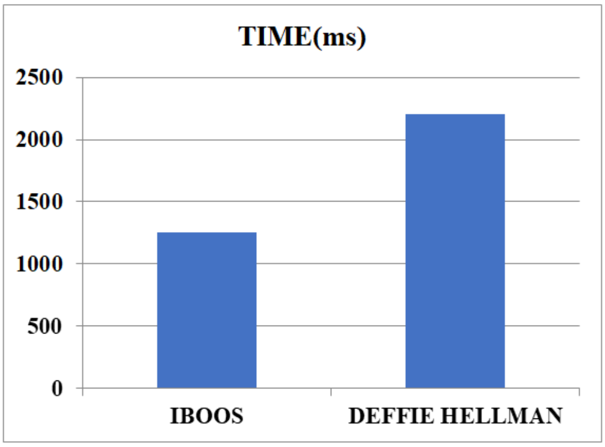


3.4 Data Replication Module

In this module the information replication is conceivable if the RSU in the vehicle adhoc network is more précised and the each RSU has its own adhocmodle where the copy records are recognized and the each copy records are broke down. The records which are coordinated with the other rsu will distinguish the information and the replication module. The every vehicle adhoc network in the rsu unit will deal with the specific vehicle adhoc network. You can utilize the Database Replication module to import information from existing data sets. Complex mappings over different table joins are likewise conceivable. You can design in the customer or from Java.

4. EXPERIMENTAL SETUP

For any circle, we discover the runtime of the square inside them and increase it by the occasions the program will rehash the circle. All circles that develop relatively to the info size make some direct memories intricacy O (n). Assuming you circle through just 50% of the exhibit, that is still O (n), Time intricacy addresses the occasions an assertion is executed. The time intricacy of a calculation isn't the real time needed to execute a specific code, since that relies upon different elements like whatever the information, this will return in a fixed, limited time. In the above intricacy the least runtime to execute the program was iboos calculation with the avg of 1250 ms, and the additional time taken to execute is deffie hellman.



Algorit	Time(Ms)
Iboos	1250
Deffie Hellman	2200

5. CONCLUSION

In this task, we proposed a compelling information access control CP-ABE plan to divide information between various application specialist co-ops and distributed storage frameworks for vehicles in a VANET. Our plan gives both client and trait disavowals by different qualities. We additionally utilized cloud process hubs to share the computational heap of encryption and decoding to offer help for asset obliged gadgets; this methodology makes CP-ABE careful the IBOOS more appropriate for VANETs. Through the far reaching security investigation and exploratory assessment results, we show that our answer keeps up with client protection as well as is secure against different assaults. Also, our plan ensures both versatility and effectiveness. In future work, we will test our plan in a genuine climate and measure the correspondence latencies between elements.

6. REFERENCES

[1] A. Juels and J. Burton S. Kaliski, “PORs: Proofs of retrievability for large files,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 584–597, ACM, 2007.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 598–609, ACM.

[3] C. Erway, A. Kupc¸ ¨ u, C. Papamanthou, and R. Tamassia, “Dynamic ¨ provable data possession,” in Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 2009, pp. 213–222, ACM, 2009.

[4] B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” in Proceedings of 5th International Conference on Cloud Computing, Cloud 2012, pp. 295–302, IEEE, 2012.

[5] J. Xu, A. Yang, J. Zhou, and D. S. Wong, “Lightweight Delegatable proofs of storage,” in Proceedings of 21st European Symposium on Research in Computer Security, ESORICS 2016, pp. 324–343, Springer International Publishing, 2016.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for secure cloud storage,” IEEE Transactions on Computers, TC 2013, vol. 62, no. 2, pp. 362–375, 2013.

[7] I. G. Aniket Kate, Gregory M. Zaverucha, “Constant-Size Commitments to Polynomials and Their Applications,” in Advances in Cryptology - ASIACRYPT 2010, pp. 177–194.