ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Processing Dynamic and Indirect Mutual Trust Data in Cloud Computing Storage

Kanumuri J S Rama Raju
Associate Consultant,
Department of CSE,
MLR Institute of Technology,
Hyderabad, India.

G Kiran Kumar
Professor,
Department of CSE,
MLR Institute of Technology,
Hyderabad, India.

Abstract:

Currently, the amount of sensitive data produced by many organizations is outpacing their storage ability. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, we propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append, (ii) it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data, (iii) it enables indirect mutual trust between the owner and the CSP, and (iv) it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

Index Terms: Outsourcing data storage, dynamic environment, mutual trust, access control.

INTRODUCTION:

Cloud computing has received considerable attention from both academia and industry due to a number of important advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, flexibility to scale up and down information technology (IT) capacity, and mobility where customers can access information wherever they are, rather than having to remain at their desks. Cloud computing is a distributed computational model over a large pool of shared-virtualized computing resources (e.g., storage, processing power, memory, applications, services, and network bandwidth). Cloud service providers (CSPs)[1] offer different classes of services (Storage-as-a-Service (SaaS), Application-as-a-Service, and Platform-as-a-Service) that allow organizations to concentrate on their core business and leave the IT operations to experts.

current world, many organizations have shifted to cloud and some of they have been shifting to cloud based system. They are producing a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, Cloud service providers (CSPs) offered Storage-asa-Service is a emerging solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage. Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote cloud server.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites.

RESEARCH OBJECTIVES:

The implementation of a cloud-based storage scheme that has the following roles:

(i)allowing a data owner to outsource the data to a CSP, and perform full at the block level operations more dynamically, i.e., it supports operations such as block modification, insertion, deletion, and append;

(ii) ensuring the newness property, i.e., the authorized users receive the most recent version of the outsourced data;[4]

(iii) developing an indirect mutual trust between the data owner and the CSP since each party resides in a different trust domain;[6] and

(iv)enabling the access control for the outsourced data.

PROBLEM STATEMENT:

Commonly, traditional access control techniques assume the existence of the data owner and the storage servers[2] in the same trust domain. This assumption, however, no longer holds when the data is outsourced to a remote CSP, which takes the full charge of the outsourced data management, and resides outside the trust domain of the data owner. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote untrusted CSP. Through this solution, the data is encrypted under a certain key, which is shared only with the authorized users. The unauthorized users, including the CSP[3], are unable to access the data since they do not have the decryption key. This general solution has been widely incorporated into existing schemes, which aim at providing data storage security on untrusted remote servers. Another class of solutions utilizes attribute-based encryption to achieve fine-grained access control . These approaches can prevent and detect malicious actions from the CSP side. On the other hand, the CSP [3]needs to be safeguarded from a dishonest owner, who attempts to get illegal compensations by falsely claiming data corruption over cloud servers. This concern, if not properly handled, can cause the CSP to go out of business

EXISTING SYSTEM:

In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, storage-as-a-service offered by cloud service providers (CSPs) emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage.Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites.

Drawbacks:

CSP needs to be safeguarded from a dishonest owner, who attempts to get illegal compensations by falsely claiming data corruption over cloud servers. This concern, if not properly handled, can cause the CSP to go out of business.

LITERATURE SURVEY:

A number of PDP protocols have been presented to efficiently validate the integrity of data,[1]-[8] e.g., Proof of retrievability was introduced as a stronger technique than PDP in the sense that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers.[9]We introduce a model for provable data possession (PDP) that allows a client that has stored data at an un-trusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage system.We present two provably-secure PDP schemes that are more efficient than

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.Provable data possession at un-trusted stores[1] Checking data possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, etc.) is a matter of crucial importance. Remote data possession checking protocols permit to check that a remote server can access an uncorrupted file in such a way that the verifier does not need to know beforehand the entire file that is being verified. Unfortunately, current protocols only allow a limited number of successive verifications or are impractical from the computational point of view. In this paper, we present a new remote data possession checking protocol such that: 1) it allows an unlimited number of file integrity verifications; 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier.Efficient remote data possession checking in critical information infrastructures[2]

Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client's (potentially very large) outsourced data. The storage server is assumed to be un-trusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, our PDP technique allows outsourcing of dynamic data, i.e, it efficiently supports operations, such as block modification, deletion and append. Scalable and efficient provable data possession[3]We consider the problem of efficiently proving the integrity of data stored at un-trusted servers.

In the provable data possession (PDP) model, the client preprocesses the data and then sends it to an un-trusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP scheme applies only to static (or append-only) files. We present a definitional framework and efficient constructions for dynamic provable data possession (DPDP) [5], which extends the PDP model to support provable updates to stored data. We use a new version of authenticated dictionaries based on rank information. The price of dynamic updates is a performance change from O(1) to O(logn) (or O(nɛlogn), for a file consisting of n blocks, while maintaining the same (or better, respectively) probability of misbehavior detection. Our experiments show that this slowdown is very low in practice (e.g. 415KB proof size and 30ms computational overhead for a 1GB file). We also show how to apply our DPDP scheme to outsourced file systems and version control systems (e.g. CVS).Dynamic provable data possession[4]

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a [6]third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public verifiability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in our protocol design.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In particular, to achieve efficient data dynamics, we improve the Proof of Retrievability model [1] by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.Enabling public verifiability and data dynamics for storage security in cloud computing[5] A distributed cryptographic system that permits aset of servers to prove to a client that a stored file is intact and retrievable. HAIL is a remote-file integrity checking protocol that offers efficiency, security, and modeling improvements over straightforward multiserver application of POR protocols and over previously proposed, distributed file-availability proposals. Through a careful interleaving of different types of error-correcting layers, and inspired by proactive cryptographic models, HAIL ensures file availability against a strong, mobile adversary.HAIL: a high-availability and integrity layer for cloud storage[6]

New cryptographic building block known as a proof of retrievability (POR). A POR enables a user (verifier) to determine that an archive (prover) "possesses" a file or data object F. More precisely, a successfully executed POR assures a verifier that the prover presents a protocol interface through which the verifier can retrieve F in its entirety. Of course, a prover can refuse to release F even after successfully participating in a POR. A POR, however, provides the strongest possible assurance of file retrievability barring changes in prover behavior. The privacy and integrity guarantees of conventional cryptography will benefit from extension into POR-based assurances around data availability.PORs: Proofs of Retrievability for large files[7].

As storage systems and individual storage devices themselves become networked, they must defend both against the usual attacks on messages traversing an untrusted, potentially public, network as well as attacks on the stored data itself. This is a challenge because the primary purpose of networked storage is to enable easy sharing of data, which is often at odds with data security. To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers. Stored data must be protected over longer periods of time than typical message round-trip times. The main feature of Plutus is that all data is stored encrypted and all key distribution is handled in a decentralized manner.Plutus provide basic filesystem security features -- (1) to detect and prevent unauthorized data modifications, (2) to differentiate between read and write access to files, and (3) to change users' access privileges. Plutus is an encrypt-on-disk system where all the key management and distribution is handled by the client.(1) protect against data leakage attacks on the physical device, such as by an untrusted administrator, a stolen laptop, or a compromised server; (2) allow users to set arbitrary policies for key distribution (and therefore file sharing); and (3) enable better server scalability because most of the computationally intensive cryptographic operations are performed at end systems, rather than in centralized servers. Cryptographic primitives applied to the problem of secure storage in the presence of untrusted servers and a desire for owner-managed key distribution. Eliminating almost all requirements for server trust (we still require servers not to destroy data - although we can detect if they do) and keeping key distribution (and therefore access control) in the hands of individual data owners provides a basis for a secure storage system that can protect and share data at very large scales and across trust boundaries.Plutus: Scalable secure file sharing on untrusted storage[8]

Fine grained data access control in cloud computing. One challenge in this context is to achieve fine grained ness, data confidentiality, and scalability simultaneously. Schemes to achieve this goal by exploiting KP ABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Enabling the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Schemes secured under standard cryptographic models.Achieving secure, scalable, and fine-grained data access control in cloud computing[9] Formal base model for the correct application of selective encryption. The model allows thedefinition of an encryption policy equivalent to the authorization policy to be enforced on the resources. We note that, while it is in principle advisable to leave authorization-based access control and cryptographic protection separate, in the outsourcing scenario such a combination can provesuccessful:

selective encryption allows selective accessto be enforced by the service provider itself without the ownerIntervention. Solutions provide protection by exploiting encryption in conjunction with proper indexing capabilities, enforcing the authorization policy by using a two-layer selective encryption.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Offers significant benefits in terms of quicker and less costly realization of authorization policy updates and general efficiency of thesystem (replication of resources can carry along the policyitself). Over-encryption: Management of access control evolution on outsourced data[10]

PROPOSED SYSTEM:

In the proposal scheme that addresses important issues related to outsourcing storagedata, namely dynamic data, newness, mutual trust, and access control. The remotely stored data cannot be only accessed by authorized users, but also updated and scaled by the owner. After updating, authorized users should receive the latest version of the data (newness property), i.e., a technique is required to detect whether the received data are stale.

Mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme. A mechanism is introduced to determine the dishonest party, i.e., misbehavior from any side is detected and the responsible party is identified. Last but not least, The design and implementation of a cloud-based storage scheme that has the following features:

- it allows a data owner to outsource the data to a CSP, and perform full dynamic operations at the block-level, i.e., it supports operations such as block modification, insertion, deletion, and append;

- it ensures the newness property, i.e., the authorized users receive the most recent version of the outsourced data;

- it establishes indirect mutual trust between the data owner and the CSP because each party resides in a different trust domain; and

- it enforces the access control for the outsourced data.

We discuss the security features of the proposed scheme. Besides, we justify its performance through theoretical analysis and a prototype implementation on Amazon cloud platform to evaluate storage, communication, and computation overheads. In this project proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity/newness, a TTP is able to determine the dishonest party. The data owner enforces access control for the out sourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme. important features of outsourcing data storage can be supported without excessive overheads in storage, communication, and computation.

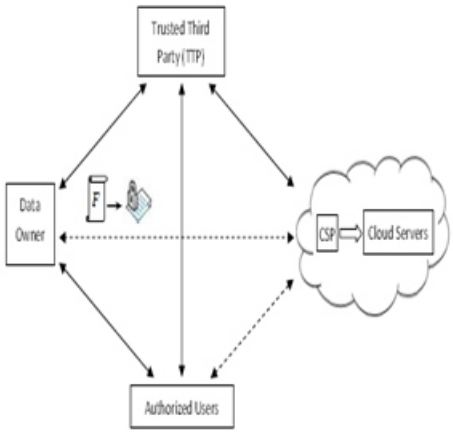
ADVANTAGES:

(i) It allows a data owner to outsource the data to a CSP, and perform full dynamic operations at the block-level, i.e., it supports operations such as block modification, insertion, deletion, and append;

(ii) It ensures the newness property, i.e., the authorized users receive the most recent version of the outsourced data;

(iii) It establishes indirect mutual trust between the data owner and the CSP since each party resides in a different trust domain; and

(iv) It enforces the access control for the outsourced data



The relations between different system components are represented by double-sided arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the dataowner, the authorized users, and the CSP trust the TTP.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to enable indirect mutual trust between these three components. There is a direct trust relation between the data owner and the authorized users.The storage model used in this work can be adopted by many practical applications. For example, e-Health applications can be envisioned by this model, where the patients' database that contains large and sensitive information can be stored on cloud servers. In these types of applications, a medical centers can be considered as the data owner, physicians as the authorized users who have the right to access the patients' medical history, and an independent-trusted organization as the TTP. Many other practical applications like financial, scientific, and educational applications can be viewed in similar settings.

Outsourcing, updating, and accessing:

The data owner has a file F consisting of m blocks to be outsourced to a CSP, where storage fees are pre-specified according to the used storage space. For confidentiality, the owner encrypts the data before sending to cloud servers. After data outsourcing, the owner can interact with the CSP to perform block-level operations on the file. These operations includes modify, insert, append, and delete specific blocks. In addition, the owner enforces access control by granting or revoking access rights to the outsourced data.

An authorized user sends a data-access request to the CSP, and receives the data file in an encrypted form that can be decrypted using a secret key generated by the authorized user (more details will be explained later). We assume that the interaction between the owner and the authorized users to authenticate their identities has already been completed, and it is not considered in this work. Moreover, all authorized users have the same privileges, i.e., the issue of access hierarchy is outside the current scope.

The TTP is an independent entity, and thus has no incentive to collude with any party in the system. However, any possible leakage of data towards the TTP must be prevented to keep the outsourced data private. The TTP and the CSP are always online, while the owner is intermittently online. The authorized users are able to access the data file from the CSP even when the owner is offline. Throughout this paper, the terms cloud server and cloud service provider are used interchangeably.

IMPLEMENTATION:
Activity Flow:

Various modules and their implementations.

Data Owner Module, In this module, we develop the data owner module, where A data owner that can be an organization generating sensitive data to be stored in the cloud and made available for controlled external use. First, the data owner has to register with the cloud service provider, to store their data in Cloud Server. After Registering, the data owners gets credential login access using their perspective username and password. The data owner then can upload their files in it. The details of uploaded files are also listed in the separate menu. All the uploaded files are encrypted securely. Only authorized users can only decrypt the file contents uploaded by the data owner.

Cloud Service Provider Module, In this module we develop the Cloud Service Provider. CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users. All the files uploaded by the data owner are saved in Cloud Server managed by the cloud service providers. We also consider, the CSP is un-trusted, and thus the confidentiality and integrity of data in the cloud may be at risk. For economic incentives and maintaining a reputation, the CSP may hide data loss, or reclaim storage by discarding data that has not been or is rarely accessed.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Authorized Users Module, we develop the authorized user module, where the authorized user is a set of owner's clients who have the right to access the remote data. Also we consider the system model; On the other hand, a data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement. They may dishonestly claim that data integrity over cloud servers has been violated, or the CSP has returned a stale file that does not match the most recent modifications issued by the owner.Trusted Third Party (TTP) Module, we develop the TTP, a trusted third party (TTP), an entity who is trusted by all other system components, and has capabilities to detect/specify dishonest parties. In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .Also ttp checks the CSP(CLOUD SERVICE PROVIDER),and find out whether the csp is authorized one or not.The primary Procedural steps for the proposed system include "Setup and File Preparation", "Dynamic Operations on the Outsourced Data", "Data Access and Cheating Detection". The Setup and File Preparation is implemented in two parts one is from owner side and the other from TTP side. The "Dynamic Operations on the Outsourced Data" are performed at block level and involves block modification, block insertion, block deletion.The "Data Access and Cheating Detection" has the verifications that are performed to the data received from the CSP and presents how authorized users get access to the outsourced file.

CONCLUSION:

Outsourcing data to remote servers has become a growing trend for many organizations to alleviate the burden of local data storage and maintenance. In this work we have studied different aspects of outsourcing data storage: block-level data dynamic, newness, mutual trust, and access control. We have proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity/newness, a TTP is able to determine the dishonest party. The data owner enforces access 27 control for the outsourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme.

REFERENCES:

[1] 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, ser. CCS '07, 2007, pp. 598–609.

[2] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.

[3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1–10.

[4] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[6] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[7] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST 03: File and Storage Technologies, 2003.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM'10, 2010, pp. 534–542.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[10] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases. ACM, 2007, pp. 123–134.

Author's:

Mr. Kanumuri J S Rama Raju is working as Lead Associate Consultant and his research interests are Algorithms, Product Engineering, System Testing, and Cloud Computing. He has got 10 years of Software Engineering Experience.

Mr. G Kiran Kumar is working as Head of Department Computer Science Engineering and his research interests are Algorithms, Networks, Mobile Computing ,Big Data and Cloud Computing. He has got 14 years of teaching
Experience.