International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Data Integrity Checking In Public Cloud and Data Uploading Using Identity Based Proxy Oriented Data

1. Mr.U.N.P.GANGADHAR RAJU,2 S.ROHITH REDDY,3. B.SAI CHARAN,4. G.RAHUL REDDY

[1]ASSISTANT PROFESSOR, [2&3&4]UG SCHOLAR,

1. gangadhar.cse.vignan@gmail.com 2. rohithreddysama11@gmail.com, 3. saicharan057@gmail.com, 4.rahulgurram791@gmail.com

VIGNAN INSTITUTE OF TECHNOLOGY AND SCIENCE Vignan Hills, Near Ramojifilm city Deshmukhi (Village), Yadadri Bhuvanagiri Dist, Telangana– 508284

ABSTARCT:

Remote data integrity checking (RDIC) enables a data storage server, says a cloud server, to prove to a verifier that it is actually storing a data owner's data honestly. To date, a number of RDIC protocols have been proposed in the literature, but most of the constructions suffer from the issue of a complex key management, that is, they rely on the expensive public key infrastructure (PKI), which might hinder the deployment of RDIC in practice. In this project, we propose a new construction of identity-based (ID-based) RDIC protocol by making use of key-holomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI based RDIC schemes. We formalize ID-based RDIC and its security model including security against a malicious cloud server and zero knowledge privacy against a third party verifier. The proposed ID-based RDIC protocol leaks no information of the stored data to the verifier during the RDIC process. The new construction is proven secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier. Extensive security analysis and implementation results demonstrate that the proposed protocol is provably secure and practical in the real-world applications.

INTRODUCTION:

Cloud garage offers accomplice on-call for know-how outsourcing carrier model, and is gaining extremely well as a result of its snap and low protection value. However, this new know-how storage paradigm in cloud brings regarding numerous difficult fashion problems which have profound have an effect on at the protection and typical performance of the general machine, considering the truth that this expertise

storage is outsourced to cloud storage vendors and cloud purchasers lose their controls at the outsourced expertise.[16] It's charming to alter cloud shoppers to affirm the integrity of their outsourced know-how and restore the first statistics inside the cloud, simply in case their expertise has been by chance corrupted or maliciously compromised with the aid of way of insider/outsider Byzantine attacks In public cloud computing, the clients save their massive understanding within the a long way flung public cloud servers. Since the hold know-how is outside of the manager of the customers, it entails the safety dangers in terms of confidentiality, integrity and comfort of understanding and repair.[17] Remote expertise integrity checking may be a primitive which can be accustomed win over the cloud clients that their knowledge place unit unbroken intact. In some unique instances, the facts proprietor is likewise confined to get admission to the general public cloud server the facts proprietor can delegate the mission of expertise process and uploading to the third birthday party, as an example the proxy. On the alternative element, the far off facts integrity checking protocol need to be lower priced on the manner to create it appropriate for capacity limited finish gadgets. Thus, supported identity-primarily based completely public cryptography and proxy public key cryptography, we are going to study ID-PUIC protocol. Cloud storage gives companion diploma on-call for records outsourcing company model, and is gaining high-quality as an end result of its physical assets and coffee protection value.[18] However, this new facts storage paradigm in cloud brings concerning several difficult style problems which have profound have an effect on the safety and average performance of the general tool, for the reason that this records storage is outsourced to cloud garage providers and cloud customers lose their controls on the outsourced statistics. It's fascinating to change cloud shoppers to verify the integrity of their outsourced facts and restore the number one records inside the cloud, simply in case their information has been by means of accident corrupted or maliciously compromised thru insider/outsider Byzantine attacks In public cloud placing, most buyers switch their statistics to Public Cloud Server (PCS) and check their far flung statistics' integrity with the aid of net. Once the consumer is a

personal supervisor, some practical problems can display up. If the supervisor is suspected of being involved into the business enterprise fraud, he is quarantined via manner of the police. Throughout the quantity of research, the supervisor is restrained to get right of entry to the community in order to shield towards collusion. But, the manager's felony organization can press on all through the amount of investigation. Once an oversized of facts is generated, who will facilitate him approach the ones statistics If those facts can't be processed definitely in time, the supervisor can face the loss of economic interest. So as to prevent the case taking area, the supervisor has been given to delegate the proxy to method its statistics, as an instance, his secretary. But, the manager won't desire others have the energy to perform the ways off facts integrity checking. Public checking can incur a few threat of unseaworthy the privateers. For example, the hold on records volume is often detected with the useful resource of the malicious verifiers. Once the uploaded information volume is specific, personal far flung information integrity checking is critical. Though the secretary has the energy to method and transfer the data for the supervisor, he however cannot take a look at the supervisor's faraway facts integrity except he is delegated by using the supervisor. While uploading documents on cloud proxy shops reproduction of file so that if files on cloud are hacked or corrupted or integrity of files isn't always make sure then those files are over again regenerate from proxy. We will be inclined to choice the secretary due to the reality the proxy of the supervisor. In PKI (public key infrastructure), some distance off statistics integrity checking protocol can carry out the certificate control. Once the manager delegates a few entities to perform the faraway statistics integrity checking, it may incur giant overheads for the cause that booster will take a look at the certificates once it assessments the remote information integrity.

2.LITERATURE SURVEY

1) Provable data possession at untrusted stores.

AUTHORS: G. Ateniese, R. C. Burns

We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted 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 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.

2) Remote data checking using provable data possession

AUTHORS: G. Ateniese, R. C. Burns

We introduce a model for provable data possession (PDP) that can be used for remote data checking: A client that has stored data at an untrusted server can 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 is lightweight and supports large data sets in distributed storage systems. The model is also robust in that it incorporates mechanisms for mitigating arbitrary amounts of data corruption.We present two provably-secure PDP schemes that are more efficient than previous solutions. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. We then propose a generic transformation that adds robustness to any remote data checking scheme based on spot checking. 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. Finally, we

conduct an in-depth experimental evaluation to study the tradeoffs in performance, security, and space overheads when adding robustness to a remote data checking scheme.

3) Proofs of retrievability for large files

AUTHORS: A.Juels, and B. S. K. Jr. Pors

In this paper, we define and explore proofs of retrievability (PORs). A POR scheme enables an archive or back-up service (prover) to produce a concise proof that a user (verifier) can retrieve target file F, that is, that the archive retains and reliably transmits file data sufficient for the user to recover F in its entirety.A POR may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file (or bitstring) F. We explore POR protocols here in which the communication costs, number of memory accesses for the prover, and storage requirements of the user (verifier) are small parameters essentially independent of the length of F. In addition to proposing new, practical POR constructions, we explore implementation considerations and optimizations that bear on previously explored, related schemes.In a POR, unlike a POK, neither the prover nor the verifier need actually have knowledge of F. PORs give rise to a new and unusual security definition whose formulation is another contribution of our work.We view PORs as an important tool for semi-trusted online archives. Existing cryptographic techniques help users ensure the privacy and integrity of files they retrieve. It is also natural, however, for users to want to verify that archives do not delete or modify files prior to retrieval. The goal of a POR is to accomplish these checks without users having to download the files themselves. A POR can also provide quality-of-service guarantees, i.e., show that a file is retrievable within a certain time bound.

4) Compact proofs of retrievability

AUTHORS: H. Shacham, and B. Waters

In a proof-of-retrievability system, a data storage center convinces a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure—that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, we give the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of

Juels and Kaliski. Our first scheme, built from BLS signatures and secure in the random oracle model, has the shortest query and response of any proof-of-retrievability with public verifiability. Our second scheme, which builds elegantly on pseudorandom functions (PRFs) and is secure in the standard model, has the shortest response of any proof-of-retrievability scheme with private verifiability (but a longer query). Both schemes rely on homomorphic properties to aggregate a proof into one small authenticator value.

5) Provable multicopy dynamic data possession in cloud computing systems

AUTHORS: A. F. Barsoum, M. A. Hasan

Increasingly more and more organizations are opting for outsourcing data to remote cloud service providers (CSPs). Customers can rent the CSPs storage infrastructure to store and retrieve almost unlimited amount of data by paying fees metered in gigabyte/month. For an increased level of scalability, availability, and durability, some customers may want their data to be replicated on multiple servers across multiple data centers. The more copies the CSP is asked to store, the more fees the customers are charged. Therefore, customers need to have a strong guarantee that the CSP is storing all data copies that are agreed upon in the service contract, and all these copies are consistent with the most recent modifications issued by the customers. In this paper, we propose a map-based provable multicopy dynamic data possession (MB-PMDDP) scheme that has the following features: 1) it provides an evidence to the customers that the CSP is not cheating by storing fewer copies; 2) it supports outsourcing of dynamic data, i.e., it supports block-level operations, such as block modification, insertion, deletion, and append; and 3) it allows authorized users to seamlessly access the file copies stored by the CSP. We give a comparative analysis of the proposed MB-PMDDP scheme with a reference model obtained by extending existing provable possession of dynamic single-copy schemes. The theoretical analysis is validated through experimental results on a commercial cloud platform. In addition, we show the security against colluding servers, and discuss how to identify corrupted copies by slightly modifying the proposed scheme.

EXISTING SYSTEM:

- Wang et al. proposed the notion of "zero knowledge public auditing" to resist off-line guessing attack.
- Yu et al. recently enhanced the privacy of remote data integrity checking protocols for secure cloud storage, but their model works only in public key infrastructure (PKI) based scenario instead of the identity-based framework.
- Wang proposed another identity-based provable data possession in multi-cloud storage.

DISADVANTAGES OF EXISTING SYSTEM:

- MHT itself is not enough to verify the block indices, which may lead to replace attack.
- A formal security model is not provided.
- But their model works only in public key infrastructure (PKI) based scenario instead of the identity-based framework

2.2 PROPOSED SYSTEM:

- In an ID-based signature scheme, anyone with access to the signer's identity can verify a signature of the signer. Similarly, in ID-based RDIC protocols, anyone knowing a cloud user's identity, say a third party auditor (TPA), is able to check the data integrity on behalf of the cloud user. Thus, public verifiability is more desirable than private verification in ID-based RDIC, especially for the resource constrained cloud users. In this case, the property of zero-knowledge privacy is highly essential for data confidentiality in ID-based RDIC protocols.
- Our first contribution is to formalize the security model of zero knowledge privacy against the TPA in ID-based RDIC protocols for the first time.
- We fill the gap that there is no a secure and novel ID based RDIC scheme to date. Specifically, we propose a concrete ID-based RDIC protocol, which is a novel construction that is different from the previous ones, by making use of the idea of a new primitive called asymmetric group key agreement.
- To be more specific, our challenge-response protocol is a two party key

agreement between the TPA and the cloud server, the challenged blocks must be used when generating a shared key, which is a response to a challenge from the TPA, by the cloud server.

- We provide detailed security proofs of the new protocol, including the soundness and zero-knowledge privacy of the stored data. Our security proofs are carried out in the generic group model.

2.3 ADVANTAGES OF PROPOSED SYSTEM:

- This is the first correct security proof of ID-based RDIC protocol. Thus, the new security proof method itself may be of independent interest.
- We show the practicality of the proposal by developing a prototype implementation of the protocol.

3.MODULES:

- Data Owner
- KGC
- TPA
- Cloud Server

Data Owner:

In Data Owner module, Initially Data Owner must have to register their detail and KGC will authorize the registration by sending Private Key through email. After successful login data Owner can upload files into cloud server. He/she can view the files that are uploaded in cloud. Data Owner will send audit request to TPA then DO receives the audit report. After receiving the report he/she can verify the files. The following are the functionalities of data owner.

- Register
- Login
- Upload files
- Send audit request
- Verify file
- Logout

KGC:

In KGC module, KGC can view all the Data owners' details. KGC will authorize data owners also KGC will send the Private Key to the users. The following are the functionalities of KGC.

- Login
- Authorize owners
- Send private key
- Logout

TPA:

In TPA module, TPA can view all the Data owners audit request details. TPA can send challenge to cloud server to generate proof.

Then cloud receives the request and sends the proof to TPA. After receiving the proof TPA will send it to the Data Owner. The following are the functionalities of TPA.

- Login
- View files
- View audit request and send to cloud
- Verify proof and send to data owner
- Logout

Cloud Server:

In Cloud Server module, Cloud server can view Audit request details. Cloud server will generate proof and send it to TPA. Cloud Server can also view the files details in the cloud server. The following are the functionalities of Cloud.

- Login
- View files
- View request and send proof
- Logout

CONCLUSION

In this project, we investigated a new primitive called identity-based remote data integrity checking for secure cloud storage. We formalized the security model of two important properties of this primitive, namely, soundness and perfect data privacy. We provided a new construction of of this primitive and showed that it achieves soundness and perfect data privacy. Both the numerical analysis and the implementation demonstrated that the proposed protocol is efficient and practical.

FUTURE SCOPE

In Cloud Computing the security challenges are part of ongoing research. Various open issues are identified as future scope.

- **Data Classification based on Security:**

  A cloud computing data center can store data from various users. To provide the level of security based on the importance of data, classification of data can be done. This classification scheme should consider various aspects like access frequency, update frequency and access by various entities etc. based on the type of data. Once the data is classified and tagged, then level of security associated with this specific tagged data element

can be applied. Level of security includes confidentiality, encryption, integrity and storage etc. that are selected based on the type of data.

- **Identity management system:**

  Cloud computing users are identified and used their identities for accessing the services. A secure trust based identity management scheme is essentially a need by all cloud service provider and users. Various issues of identity management system are identified. Solution to secure id-generation and distribution, storage and life cycle management is a demand for trust based identity management system.

- **Secure trust based Solution for cloud computing Service:**

  A secure environment for execution of the cloud computing services along with overall security considerations is a challenge. A secure and trusted solution is the requirement that needs to be focused and addressed by the cloud computing infrastructure.

- **Optimization of resource Utilization:**

  Security considerations and provisions for virtualization along with the optimum use of the cloud infrastructure also needs to be focused and addressed.

REFERENCES:

- P. Mell, T. Grance, Draft NIST working definition of cloud computing, Reference on June. 3rd, 2009.

http://csrc.nist.gov/groups/SNC/cloudcomputing/index.html.

- Cloud Security Alliance. Top threats to cloud computing. http://www.cloudsecurityalliance.org, 2010.

- M. Blum, W. Evans, P.Gemmell, S. Kannan, M. Naor, Checking the correctness of memories. Proc. of the 32nd Anual Symposium on Foundations fo Vomputers, SFCS 1991, pp. 90–99, 1991.

- G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, D. X. Song, Provable data possession at untrusted stores. ACM Conference on Computer and Communications Security, 598-609, 2007.

- G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.

- A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc. of CCS 2007, 584-597, 2007.

- H. Shacham, and B. Waters, Compact proofs of retrievability. Proc. Of Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.

- G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphic identification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009.

- F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015.

- J. Yu, K. Ren, C.Wang, V. Varadharajan, Enabling cloud storage auditing with key-exposure resistance, IEEE Trans. on Information Forensics and Security, 10(6): 1167–1179, 2015.

- J. Liu, K. Huang, H. Rong, H. M. Wang, Privacy-preserving public auditing for regenerating-code-based cloud storage, IEEE Trans. On Information Forensics and Security, 10(7): 1513–1528, 2015.

- Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing. Proc. of ESORICS2009, LNCS 5789, 355–370, 2009.
- Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing. Proc of IEEE INFOCOM 2010, 525–533, 2010.
- Wang, K. Ren, W. Lou, and J. Li, Toward publicly auditable secure cloud data storage services. IEEE Network, 24, 19-24, 2010.
- Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, Enabling public audibility and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst., 22, 847-859, 2011.
- Wang, S. S.Chow, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for secure cloud storage. IEEE Trans. on Computers, 62, 362-375, 2013.
- K. Yang, and X. Jia. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Trans. on Parallel and Distributed Systems, 24(9): 1717-1726, 2013.