Secured Cloud Service Selection using Merkle-B Cloud Tree Indexing Strategy

KETURU MADAN MOHAN
Research Scholar,
Department of Computer Science and Engineering,
Jawaharlal Nehru Technological University Hyderabad,
(JNTUH), Kukatpally,,Hyderabad, 500085,
Telangana State, India..
Mail-id: madan.keturu@gmail.com,
ganga.madan@gmail.com.

DR.P.PREMCHAND
Professor,
Department of Computer Science and Engineering
University College of Engineering,
Osmania University, Hyderabad-500007,
Telangana State, India.
Mail-id: profpremchand.p@gmail.com.

Abstract—Cloud brokers have been recently introduced as an additional computational layer to facilitate cloud selection and service management tasks for cloud consumers. However, existing brokerage schemes on cloud service selection typically assume that brokers are completely trusted, and do not provide any guarantee over the correctness of the service recommendations. The main motto of this system is to provide the trusted cloud and easily accessible environment to users to maintain and retrieve their data in more efficient manner. This paper introduced a new algorithm called, Merkle-B-Cloud Tree Infrastructure (MBCTI), in which it is used to maintain the data in trusted manner. The Cloud Service Provider (CSP) is responsible for all transactions into the cloud environment, but that CSP doesn't have an ability to check other's data presented into the cloud. An end-to-end security is highly concentrated via integrated Authentication methodologies over this paper. Cloud brokers have been recently introduced as an additional computational layer to facilitate cloud selection and service management tasks for cloud consumers. But existing brokerage schemes on cloud service selection typically assume that brokers are completely trusted and do not provide any guarantee over the services. For all in this system users can securely maintain and retrieve the data without any interruptions.

***Index Terms*—Cloud Service Selection, Merkle-B, Tree, Data Indexing, Privacy.**

I. INTRODUCTION

Cloud Services offer a scalable variety of storage space and computing capabilities, which are widely employed by an increasing number of business owners. This has resulted in a large number of cloud service providers (CSPs), offering a wide range of resources. The availability of various, possibly complex options, however, makes it difficult for potential cloud clients to weigh and decide which options suit their requirements the best. The challenges are twofold: (a) It is hard for cloud clients to gather information about all the CSPs available for their selections; (b) It is also computationally expensive to choose a suitable CSP from a potentially large CSP pool. In light of these difficulties, both industry and academia suggested introducing an additional computing layer (referred to as cloud brokerage systems) on top of the base service provisioning to enable tasks such as discovery, mediation and monitoring. In a cloud brokerage system, one of the most fundamental tasks is to provide high-quality selection services for clients. That is, a broker provides clients with a list of recommended CSPs that meet the clients' needs. With the aid of cloud brokers, clients no longer need to collect, search or compare CSPs' services and capabilities.

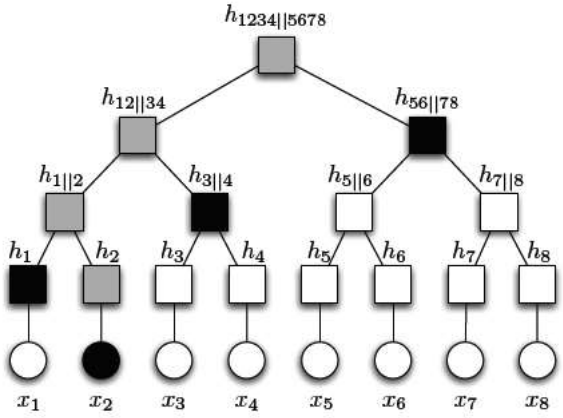


Fig.1 Merkle-B Hash Tree Model

The underlying assumption in the existing cloud brokerage schemes is that brokers are completely trusted and thus will always provide unbiased best available options to clients. Under this assumption, none of the existing works provides guarantees over the correctness or completeness of the service selection recommendations to the cloud clients. Without the ability to verify the correctness of the service recommendation, cloud clients could be easily cheated by malicious brokers. For instance, malicious brokers could recommend their favorable CSPs as much as possible and ignore other suitable CSPs, without being caught by the clients. More seriously, due to the lack of supervision and verification of brokers' actions, malicious brokers could even recommend malicious CSPs which collect and sell clients' private resources, monitor clients' hosts during cloud service provisioning, causing major financial and confidentiality losses to the clients. Therefore, it is important to equip the clients with verification capabilities of the obtained recommendations. The clients may not need to verify each recommendation result, but they certainly need to have the ability to do so when they feel necessary. In this work, we propose innovative authenticated index structures and verification protocols to allow clients to verify the completeness and authenticity of brokers' answers. This problem is related to that of authentication of query results for outsourced databases.

However, the characteristics of cloud service selection actually raise a new series of challenges. First, cloud service selection typically allows cloud users to specify multiple service requirements (i.e., multi-dimensional range queries), whereas many existing works on query authentication only support range queries on one or two dimensions (e.g., verifying location-based query results). Second, it is always desirable to have efficient cloud service selection and verification so that the cloud end users would not feel delay of services, but existing few works, although support authentication of multi-dimensional query results, are time consuming, resulting that they could not meet the demands of today's real-time cloud service recommendations. In order to overcome the limitations of existing techniques, both in terms of efficiency and supported functionality, we propose a new authenticated index structure, called Merkle-B Cloud Tree, which is a variant of the Merkle B+ tree and is specifically tailored for cloud service selections.

II. Related Study

In the year of 2010, the authors "O. Goldreich and R. Ostrovsky [1]" proposed a paper titled "Software Protection and Simulation on Oblivious Rams [1]", in that they described such as: Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM. A machine is oblivious if the sequence in which it accesses memory locations is equivalent for any two inputs with the same running time. For example, an oblivious Turing Machine is one for which the movement of the heads on the tapes is identical for each computation. (Thus, the movement is independent of the actual input.) What is the slowdown in the running time of a machine, if it is required to be oblivious? In 1979, Pippenger and Fischer showed how a two-tape oblivious Turing Machine can simulate, on-line, a one-tape Turing Machine, with a logarithmic slowdown in the running time. We show an analogous result for the random-access machine (RAM) model of computation. In particular, we show how to do an on-line simulation of an arbitrary RAM by a probabilistic oblivious RAM with a polylogaithmic slowdown in the running time. On the other hand, we show that a logarithmic slowdown is a lower bound.

In the year of 2012, the authors "D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano [2]" proposed a paper titled "Public key encryption with keyword search [2]", in that they described such as: the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

In the year of 2010, the authors "S. Kamara and K. Lauter [3]" proposed paper titled "Cryptographic cloud storage in Financial Cryptography and Data Security [3]", in that they described such as: the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

III. System Summary

A. Existing System

Cloud services offer a scalable variety of storage space and computing capabilities, which are widely employed by an

increasing number of business owners. This has resulted in a large number of cloud service providers (CSPs), offering a wide range of resources. The availability of various, possibly complex options, however, makes it difficult for potential cloud clients to weigh and decide which options suit their requirements the best. The challenges are twofold: It is hard for cloud clients to gather information about all the CSPs available for their selections. It is also computationally expensive to choose a suitable CSP from a potentially large CSP pool. Existing works on cloud service selection are focused only on how to select the services that satisfy customers' requirements. None of them considers security issues involved in the service selection, and none of them provides verifiable schemes to prove the correctness and completeness of their service selection results as addressed in our work.

Disadvantages

- Fully Broker based data maintenance methodology and data are open to server administrator.
- Existing works on cloud service selection are focused only on how to select the services that satisfy customers' requirements.
- None of them considers security issues involved in the service selection, and none of them provides verifiable schemes to prove the correctness and completeness of their service selection results as addressed in our work.

B. Proposed System

Existing use the collector for securely generating and sharing location-based information, whereas, we use the collector to achieve service verification in the cloud. Our proposed authenticated index structures are related to those developed for query authentication in outsourced databases which can be classified into two main categories: Hash-based approaches and Signature-based approaches. As our proposed data structure is developed based on the Merkle-B tree indexing strategy.

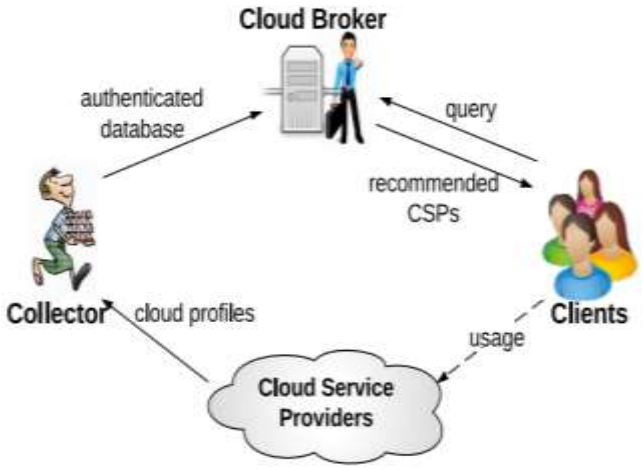


Fig.2 Proposed System Architecture

Advantages

- Broker free trusted data maintenance service.
- CSP cannot able to view the Server data.
- Cost, Time and Performance is so effective.

The following algorithm illustrates the proposed system logic and the flow nature in detail.

Algorithm: Merkle Hash Tree

Step-1: Take a file or stream of binary data
Step-2: Split the file into chunks, not necessarily of the same size, but usually the case
Step-3: For an odd number of chunks, use an all-zeros value to complete the pair
Step-4: Generate a hash digest, e.g. SHA1, of each chunk
Step-5: Arrange these in the same order as the content in the file
Step-6: Interleave an empty space after each chunk hash, for subsequent hashes
Step-7: Optionally, these can be inserted into an array using the even indexes
Step-8: Concatenate each pair of chunk hashes, and hash the resulting data again with SHA1
Step-9: Move "up" a row, or level, in the tree-to-be
Step-10: Insert the new hash digest in the spare slot between the two hashed chunks
Step-11: Repeat across the whole file
Step-12: Between each pair of original chunks, there will still be a spare slot left
Step-13: Move "up" a level in the tree again

Step-14: This time, hash the hash digests from the second layer, not the bottom layer
Step-15: Repeat this process using only the newly generated hashes, across the whole file
Step-16: Finally, repeat this entire process until there is a single hash digest of the entire file.

IV. SYSTEM IMPLEMENTATION

This paper adopts the new methodologies and those methodologies are implemented by using the following modules, which are all will be briefly explained below.

A. Cloud Service Provider Portal

This Cloud Service Provider Portal module is the Main Portal for Cloud Service Provider, which provides an ability to the CSP to navigate to the respective pages such as Cloud Server Creation, Registration Accept/Removal and File Maintenance Portal. Generally says, a cloud Service provider is a company or individual, which offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. Cloud providers are sometimes referred to as cloud service providers or CSPs.

B. Authentication Module

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. User authentication is the verification of an active human-to-machine transfer of credentials required for confirmation of a user's authenticity; the term contrasts with machine authentication, which involves automated processes that do not require user input.

C. User Verification Module

The User Verification Module is to easily configure permissions and anything else; the verification process is role-based. New users optionally obtain a quarantine role, which can be used for evaluation, observation or simply for confusion and ambiguities. This module allows you to have e-mail verification and in meanwhile allowing the users to type their own passwords. If they do not verify their accounts in a certain time interval the user will be blocked.

D. Cloud Broker Authorization

Cloud Broker Authorization module allows the brokers to register their identities into the system with proper nature. Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.

E. Data Uploading

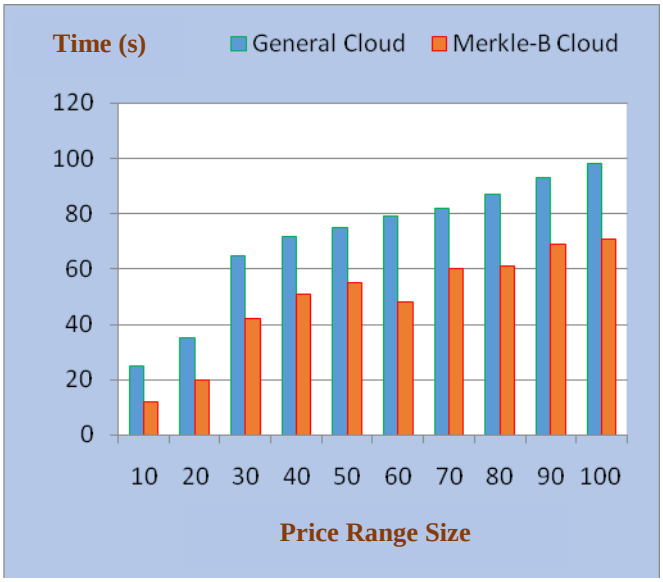
This Data Uploading module allows the data owner to upload the data into Cloud Server without any security issues. It allows the data owner to maintain their files into server with proper descriptions. Uploading is the transmission of a file from one computer system to another, usually larger computer system. From a network user's point-of-view, to upload a file is to send it to another computer that is set up to receive it.

F. Data Searching Portal

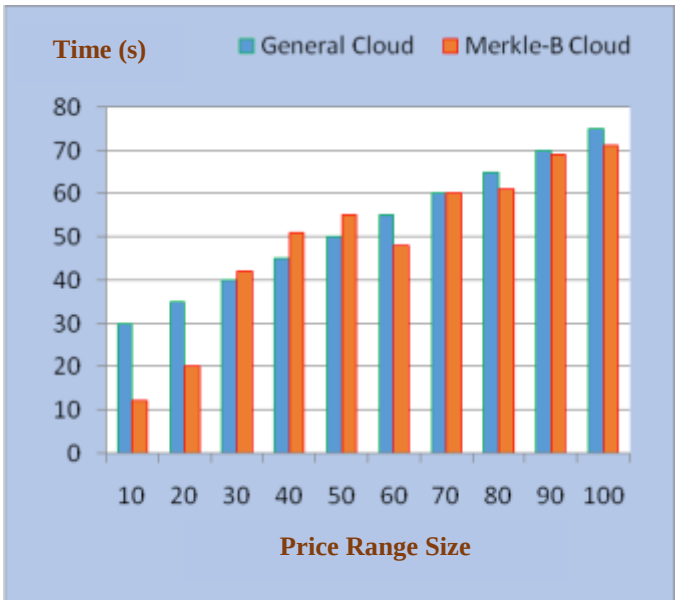
The module of Data Searching allows the data user to search for the required data from the cloud and get access from the server immediately with proper security norms. This portal is efficient for searching the data from server with advanced content based searching mechanisms.

V. RESULT AND DISCUSSION

This section briefly describes the results of the proposed approach and the algorithms are depicted with proper accuracy ratio. The proposed system algorithms Merkle-B Tree indexing nature over cloud system provides multiple features and in association with security norms. The following figure, Fig.3 provides the price range variations of the queried structure over cloud environment.



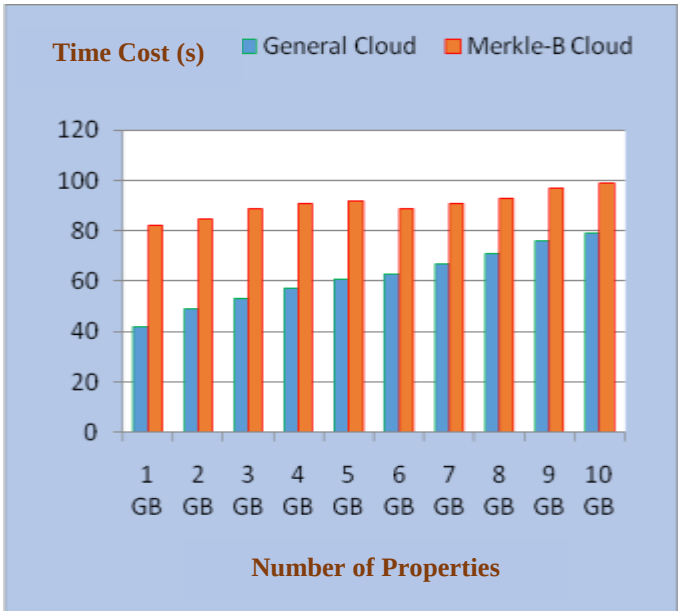
(a) Cloud Service Selection



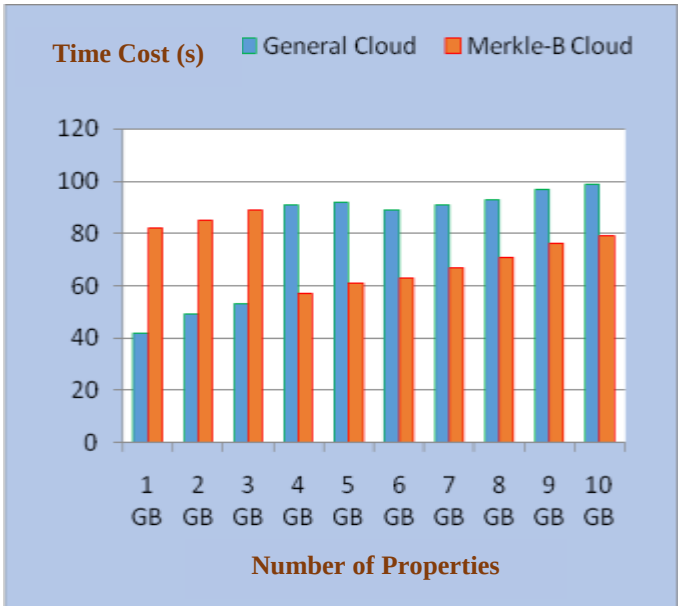
(b) Verification of Outcome

Fig.3 Effect of the Queried Price Range

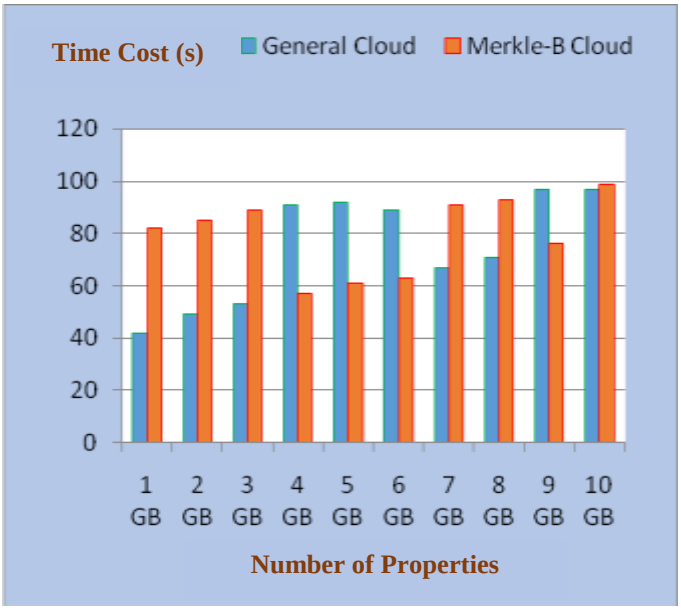
The following figure, Fig.4 illustrates that the verification performance of the proposed scheme (as shown in Fig. 4(b)), which is similar to the service selection.



(a) Server Construction



(b) Service Selection



(c) Outcome Verification

Fig.4Effect of the Cloud Service Provider Properties

VI. CONCLUSION

In this system, we propose an innovative Cloud Service Selection Verification (CSSV) system to achieve cheating-free cloud service selection under cloud brokerage architecture. The core of our system is an efficient authenticated index structure to ensure the authenticity, the satisfiability and the completeness of the service selection results. Our experimental results show the effectiveness and efficiency of our schemes compared with the state-of-the-art.

References

[1] O. Goldreich and R. Ostrovsky, "Software Protection and Simulation on Oblivious Rams", Journal of the ACM, https://doi.org/10.1145/233551.233553, 2010.
[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search", International Conference on the Theory and Applications of Cryptographic Techniques, 2012.
[3] S. Kamara and K. Lauter, "Cryptographic cloud storage in Financial Cryptography and Data Security", International Conference on Financial Cryptography and Data Security, 2010.
[4] A. Lenk, M. Menzel, J. Lipsky, S. Tai, and P. Offermann, "What are you paying for? performance benchmarking for Infrastructure-asa-Service offerings," in 2011 IEEE International Conference on Cloud Computing (CLOUD), 2011, pp. 484–491.
[5] Z. urRehman, O. K. Hussain, S. Parvin, and F. K. Hussain, "A framework for user feedback based cloud service monitoring," in 2012 Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), 2012, pp. 257–262.
[6] L. Li and Y. Wang, "Subjective trust inference in composite services." AAAI, 2010.
[7] L. Qu, Y. Wang, and M. A. Orgun, "Cloud service selection based on the aggregation of user feedback and quantitative performance assessment," in 2013 IEEE International Conference on Services Computing (SCC), 2013, pp. 152–159.
[8] L. Xin and A. Datta, "On trust guided collaboration among cloud service providers," in 2010 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010, pp. 1–8.
[9] S. Sundareswaran, A. Squicciarini, and D. Lin, "A brokerage-based approach for cloud service selection," in 2012 IEEE 5th International Conference on Cloud Computing (CLOUD). IEEE, Aug. 2012, pp. 558–565.
[10] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in SIGMOD '06: Proceedings of the 2006 ACM SIGMOD international conference on Management of data. ACM Request Permissions, Jun. 2006.
[11] E. Mykletun, M. Narasimha, and G. Tsudik, "Signature bouquets: immutability for aggregated/condensed signatures," in Computer Security – ESORICS 2004, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, vol. 3193, pp. 160–176.
[12] M. Narasimha and G. Tsudik, "DSAC: integrity for outsourced databases with signature aggregation and chaining," in Proceedings of the 14th ACM International Conference on Information and Knowledge Management, 2005, pp. 235–236.
[13] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data, 2005, pp. 407–418.
[14] H. Pang, J. Zhang, and K. Mouratidis, "Scalable verification for outsourced dynamic databases," Proceedings of the VLDB Endowment, vol. 2, no. 1, pp. 802–813, 2009.
[15] Q. Zheng, S. Xu, and G. Ateniese, "Efficient query integrity for outsourced dynamic databases," in CCSW '12 Proceedings of the 2012 ACM Workshop on Cloud computing security workshop. ACM, 2012, pp. 71–82.
[16] Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios, "Authenticated indexing for outsourced spatial databases," The VLDB Journal, vol. 18, no. 3, pp. 631–648, 2009.
[17] P. Devanbu, M. Gertz, C. Martel, and S. G. Stubblebine, "Authentic data publication over the internet," Journal of Computer Security, vol. 11, no. 3, pp. 291–314, 2003.
[18] W. Cheng, H. Pang, and K.-L. Tan, "Authenticating multidimensional query results in data publishing," in Proceedings of the 20th IFIP WG 11.3 Working Conference on Data and Applications Security, 2006, pp. 60–73.
[19] H. Pang and K.-L. Tan, "Authenticating query results in edge computing," in Proceedings of the 20th International Conference on Data Engineering (ICDE), 2004, pp. 560–571.
[20] Z. Yang, S. Gao, J. Xu, and B. Choi, "Authentication of range query results in mapreduce environments," in Proceedings of the Third International Workshop on Cloud Data Management, 2011, pp. 25–32.
[21] H. V. Jagadish, B. C. Ooi, K.-L. Tan, C. Yu, and R. Zhang, "iDistance: an adaptive B+-tree based indexing method for nearest neighbor search," ACM Trans Database Systems (TODS), vol. 30, no. 2, pp. 364–397, Jun. 2005.
[22] S. Papadopoulos, D. Papadias, W. Cheng, and K.-L. Tan, "Separating authentication from query execution in outsourced databases," in IEEE 25th International Conference on Data Engineering (ICDE), 2009, pp. 1148–1151.
[23] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM Transactions on Storage (TOS), vol. 2, no. 2, pp. 107–138, 2006.
[24] S. Bajaj and R. Sion, "CorrectDB: SQL engine with practical query authentication," Proceedings of the VLDB Endowment, vol. 6, no. 7, pp. 529–540, 2013.

[25] D. Papadopoulos, S. Papadopoulos, and N. Triandopoulos, "Taking authenticated range queries to arbitrary dimensions," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 819–830.