International Journal of Information Technology and Management
Vol. XI, Issue No. XVII, November-2016, ISSN 2249-4510

A Survey on Data Security Approach for Protection in Cloud Using Attribute

Abhijit Trimbak Parchure[1]* Dr. Suneel Kumar[2]

[1]Ph.D. Research Student, MUIT, Lucknow

[2]Research Guide, MUIT, Lucknow

Abstract – Cloud computing has turned into a standout amongst the most critical data security issue lately. That is because of the breathtakingly developing applications and obliged services of cloud computing. Notwithstanding, with a specific end goal to securely use and revel in the profit of cloud computing through wired/wireless networking, sufficient confirmation of data security, for example, classified ness, verification, non-repudiation, and respectability is the most basic component for reception. Data that was once housed under the security realm of the service client has now been put under the insurance of the service provider. Clients have lost control over the security of their data. The proposed approach combines the fine-grained access control and keyword search encryption to provide multiple users' access controls in the cloud environment with encrypted data protection. The user in this situation can retrieve the data file from the cloud database only if she/he gives appropriate keywords and presents the identity or position that satisfies the rules of the access rights.

As Cloud Computing gets to be pervasive, delicate data are as a rule progressively brought together into the cloud. For the security of information protection, delicate information must be encoded before outsourcing, which makes powerful information usage an extremely difficult assignment. Albeit customary searchable encryption plans permit clients to safely seek over encoded information through watchwords, these systems bolster just Boolean inquiry, without catching any significance of information records. This approach experiences two fundamental downsides when straightforwardly connected with regards to Cloud Computing.

Keywords: Data Security, Approach, Protection, Cloud Computing, Attribute, etc.

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

INTRODUCTION

In this study, interestingly we characterize and take care of the issue of viable yet secure positioned keyword seeks over scrambled cloud information. Positioned look significantly improves framework ease of use by giving back the coordinating records in a positioned arrange with respect to certain importance criteria (e.g., watchword recurrence), consequently making one stage nearer towards reasonable organization of security safeguarding information facilitating administrations in Cloud Computing. We first give a clear yet perfect development of positioned watchword seek under the best in class searchable symmetric encryption (SSE) security definition, and exhibit its wastefulness. To accomplish more pragmatic execution, we then propose a definition for positioned searchable symmetric encryption, and give a proficient plan by legitimately using the current cryptographic primitive, arrange protecting symmetric encryption (OPSE). Careful investigation demonstrates that our proposed arrangement appreciates "as-solid as would be prudent" security ensure contrasted with past SSE plans, while accurately understanding the objective of positioned watchword look.

Extensive experimental results demonstrate the efficiency of the proposed solution. Cloud computing is an emerging paradigm offering companies (virtually) unlimited data storage and computation at attractive costs. It is a cost-effective model because it does not require deployment and maintenance of any dedicated IT infrastructure. Despite its benefits, it introduces new challenges for protecting the confidentiality of the data. Sensitive data like medical records, business or governmental data cannot be stored unencrypted on the cloud. Companies need new mechanisms to control access to the outsourced data and allow users to query the encrypted data without revealing sensitive information to the cloud provider.

State-of-the-art schemes do not allow complex encrypted queries over encrypted data in a multi-user setting. Instead, those are limited to keyword searches or conjunctions of keywords. This research

extends work on multi-user encrypted search schemes by supporting SQL-like encrypted queries on encrypted databases. Furthermore, we introduce access control on the data stored in the cloud, where any administrative actions (such as updating access rights or adding/deleting users) do not require re-distributing keys or re-encryption of data. Finally, we implemented our scheme and presented its performance, thus showing feasibility of our approach.

REVIEW OF LITERATURE:

Cloud computing could be regarded to a specific degree, as the progression of framework processing. Such a close relationship has started perplexity. The grid composition is at first dictated by exploratory purposes, and pointed at sorting out assets that are not subject to unified control under standard, open, generally helpful traditions and interfaces (Foster et al,2008). Cloud computing is imagined for business purposes and normally benefit arranged. It depends on concentrated server farms. The traditions and interfaces used may not be the same across over mists suppliers.

Cloud computing has absolutely divergent arrangement of activity. It offers clear Slas (Service Level Agreements) and depends on a "pay for each use" assessing model (Wang, et. al., 2011). Along these lines it is ensured that with just accredit card, one can get on-demand access to 100,000+ processors from the mists (Foster et al., 2008). Grid computing on the other hand depends on an offering framework, that is, one needs to join the structure and contribute computing energy to expand access to the registering power of various parts. In this co-specialist display, Slas are not obliged or enforceable (Gentry, 2009. Barbosa and Farshim, 2011. Benabbas, et. al., 2011) in this study, we see cloud computing depends on "a far reaching pool of adequately usable and open virtualized assets, (for instance, equipment, progression stages or administrations)" (Boneh and Franklin, 2003). These assets are ordinarily inalienable brought together server farms and are alterably re-orchestrated to achieve an optimum utilization. Mists are outfitted by a compensation as-you-go show in which sureties are offered by the supplier's by means of revamped Slas (Service Level Agreements). This changes registering power into an open utility which will convey a critical "standard change" to the IT business and even to social request all in all cloud computing has ensured various creative and sociological benefits. The processing force is created from incredibly brought together and organized server farms which hold up to a colossal number of servers, with an extensive economy of scale. From a wander edge, cloud computing can pass on-request figure power at a very low if no cost of the direct establishment and advancing upkeep. Cloud computing is like manner certifications to outfit better execution, trustworthiness and adaptability (Goyal, et. al., 2006). There is some affirmation that these are constantly passed on, (Katz, et. al., 2008). From an ecological position, attributable to the progressed electrical and cooling frameworks used by its brought together server farms, cloud computing has ensured to convey low natural cost and high life adequacy, appeared differently in relation to the all-inclusive scattered undertaking server farms (Catteddu and Hogben, 2009). With everything considered, these charming assurances have drawn profoundly extending thought of an overall scale.

The degree that the security issue for information relocation is concerned, the distinctive cryptographic procedures have been used earlier, for instance, Identity Based Encryption (IBE), Attribute Based Encryption (ABE) and Prediction based Encryption (PBE) in Identity Based system, an uncommon identifier of the beneficiary, for instance, message address is used for finding out the general population key by the unprejudiced assembling servers. This framework is generally used for multicasting and is started from both Identity Based encryptions (IBE) and Attribute Based Encryption (ABE). While in IBE method, character of a component is used for encryption key and unscrambling key as well, the PBE (estimate based encryption) technique is vastly improved arrangement as the personality of a substance is resolved from an arranged of characteristics and for decoding, get to strategies are there. It joins going with four stages for performing encryption, unscrambling and delivering key. a) Setup: to create a riddle key that exhibits as an expert key, for delivering decoding key and an arrangement of open parameters. b) Keygen: a decoding key is created by using this operation's) Encrypt: this operation plays out the encryption of plain substance with the assistance of open parameters and supplied encryption keyed) Decrypt: is used for unscrambling the figure text.in along these lines, Prediction Based Encryption strategy ended up being feasible for giving security of information in cloud. Be that as it may, in any case it neglects to offer a more capable part to make information security more grounded and taking care of the work immovable quality. Along these lines, in this study we proposed an approach of using randomization and making an enhanced encryption procedure to improve the security of information relocation handle in cloud.

1. **Cloud Computing:** Cloud computing is a developing worldview offering outsourced administrations to undertakings for putting away and preparing an enormous measure of information at exceptionally focused expenses. It guarantees higher accessibility, versatility and more compelling nature of administration than in-house arrangements. In cloud computing, the outsourced bit of information is inside simple reach of cloud administration suppliers. Tragically, one of the solid snags in far reaching reception of

the cloud is to save privacy of the information. There are a few strategies that can ensure classification of information put away in outsourced situations while supporting fundamental hunt capacities. Be that as it may, they don't bolster get to control approaches to manage access to a specific subset of the put away information (Menascé and Ngo, 2009). Best in class arrangement based systems can work just when they are sent and worked inside a trusted space. In an untrusted situation, get to approaches may uncover delicate data about the information they expect to ensure.

To see how get to strategies may uncover touchy data in outsourced situations, let us envision a situation where a medicinal services supplier has outsourced its wellbeing record administration administrations to an outsider administration supplier. In this situation, we don't believe the administration supplier to protect information privacy. Consequently, we can encode wellbeing records before putting away them in the outsourced environment. Besides, wellbeing records are connected with a get to approach to keep any unintended get to. Give us a chance to consider the accompanying access approach: just a Cardiologist may get to the wellbeing record, which is appended to the wellbeing record. Regardless of the possibility that the information is scrambled, an inquisitive administration supplier may at present gather private data about the patient's restorative conditions. In the illustration arrangement, an inquisitive administration supplier may effectively conclude that the patient could have heart issues. A getting out of hand administration supplier may offer this data to banks that could deny the patient an advance given her wellbeing conditions.

2. **Opportunistic Networks:** Astute systems are a rising worldview that has empowered people and undertakings to offer new administrations momentarily. The principal purpose for this adaptability is that this worldview goes for giving administrations without requiring any in-house Information Technology (IT) foundation. Essentially, pioneering systems wipe out the need of any Internet availability.

In crafty systems, hubs can distribute their own substance and subscribe to others' substance by demonstrating their advantage. Any hub can likewise go about as a specialist (additionally called a transfer) that entrepreneurially gets substance and intrigue, matches them and perhaps conveys that substance to different hubs. These astute systems could be connected to the trading of data in an extensive variety of spaces from online networking to military applications. Like cloud administration suppliers, unapproved representatives in artful systems may induce private data from clear text strategies notwithstanding when substances are encoded. Give us a chance to consider a war zone situation where fighters are occupied with sharing or securing touchy data. We accept that there is no Internet availability in the war zone. Nonetheless, warriors can trade data by means of the short-run correspondence offered by cell phones. Fighters can distribute their substance and subscribe for substance of their advantage. There are officers, known as representatives, who trade content starting with one place then onto the next. In any case, those officers must not have the capacity to access content. For directing access to content, an officer, who is distributing, can encode content utilizing best in class encryption systems and indicate a get to approach depicting which gathering of troopers can get to. For example, the arrangement could be either a Soldier from the Infantry unit or a Major can get to. Despite the fact that the substance is encoded, warriors serving as dealers and assailants (adversary having entry to cell phones of intermediaries), may surmise private data from clear text arrangements, i.e., who will get this substance. Moreover, membership data (containing enthusiasm of endorsers) may trade off security of supporters.

3. **The System and Threat Model:** We consider a cloud information facilitating administration including three unique substances, as showed in Fig. 1: information proprietor (O), information client (U), and cloud server (CS). Information proprietor has a gathering of n information records C = (F1, F2, . . ., Fn) that he needs to outsource on the cloud server in encoded shape while as yet keeping the capacity to hunt through them down successful information use reasons. To do so, before outsourcing, data owner will first build a secure searchable index I from a set of m distinct keywords W = (w1, w2, ...,wm) extracted2 from the file collection C, and store both the index I and the encrypted file collection C on the cloud server. We expect the approval between the information proprietor and clients is suitably done. To hunt the scrape accumulation down a given keyword w, an approved client creates and presents an inquiry ask for in a mystery shape—a trapdoor Tw of the watchword w—to the cloud server. After accepting the hunt ask for Tw, the cloud server is mindful to seek the file I and give back the relating set of documents to the client.

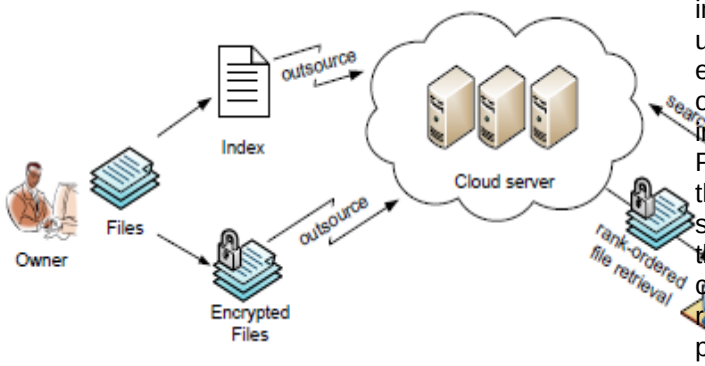

Fig. 2.1: Architecture of the search over encrypted cloud data

We consider the safe positioned watchword seek issue as takes after: the query output ought to be returned by positioned pertinence criteria (e.g., keyword recurrence based scores, as will be presented in the blink of an eye), to enhance document recovery exactness for clients without earlier information on the record gathering C. Be that as it may, cloud server ought to learn nothing or minimal about the importance criteria themselves as they display noteworthy touchy data against watchword security. To decrease data transfer capacity, the client may send a discretionary esteem k alongside the trapdoor Tw and cloud server just sends back the top-k most significant records to the client's intrigued watchword w. We consider a "legitimate yet inquisitive" server in our model, which is predictable with the greater part of the past searchable encryption plans. We accept the cloud server acts in a "genuine" mold and accurately take after the assigned convention particular, however is "interested" to gather and break down the message stream got amid the convention in order to take in extra data (Santos, et. al., 2009). As it were, the cloud server has no goal to effectively change the message stream or upset some other sort of administrations.

4. **Privacy Requirements:** Data privacy is to prevent the cloud server from prying into outsourced documents, and can be well protected by existing encryption schemes and access control mechanism. In related works on privacy-preserving query, such as searchable encryption, representative privacy requirement is that the server should learn nothing but query results. With this general privacy statement, we explore and establish a set of stringent privacy requirements specifically for our schemes.

Plaintext Privacy With respect to the plaintext privacy, if the cloud server deduces any association between frequent keywords and encrypted dataset from outsourced indices, it may learn the main content of a document. Therefore, searchable indices should be constructed in such a way that prevents the cloud server from performing such kind of association attack. This concept is identical to the plaintext privacy in. However in our setting, due to the modification of the index structure, the server may know the number of underlying keywords from the sequence of the encoded index. But the server cannot deduce any other information about keywords from the encoded indices and this leakage is tolerated in practice. Predicate Privacy Data user usually prefer to keep their query from being exposed to others like the cloud server, and the most important concern is to hide what they are querying, i.e., the keyword indicated by the corresponding token. In our ESSE schemes, the randomized generation of token can guarantee the privacy of queried keyword, which is called predicate privacy in.

5. **Protected Virtualization in Cloud Computing:** In this segment we analyze a few hazardous issues identified with cloud computing which if explained, could conceivably positively affect the appropriation of cloud computing all in all and IaaS specifically. Of the three fundamental sorts of cloud computing portrayed before (IaaS, PaaS, SaaS), IaaS overs the broadest client control over the processing stack. Such wide client control (and thus straightforwardness, from the client's perspective) gives the devices to address a few of the worries in regards to reception of open cloud computing administrations, specifically \traceability and straightforwardness inside cloud computing", and also \lack of data about the calculations behind treatment of VM pictures".

CONCLUSION:

Cloud Computing embodies the as-a-Service paradigm and allows for services to be provided en masse to consumers. When combined with the cloud setting, two different sets of scenarios emerged based upon whether the service user's or CSP's data was to be protected. PBE schemes can be used to protect service user's data in three different scenarios: Scenario I saw the inclusion of PBE within a service; Scenario II saw the provision of PBE asa-Service; and Scenario V saw PBE being deployed by the user themselves. In each of these three scenarios PBE can be used by service users to specify precisely with whom they wish to share their data, for what purpose, and for how long. Although Scenario V may be a privacy zealot's ideal choice, they are in full control its practical feasibility has yet to be determined. The staying two situations, then again, do seem, by all accounts, to be additionally encouraging. Be that as it may, these situations in themselves do exhibit a quandary amongst ease of use and ensures made over end-to-end security. At the point when hoping to ensure CSP's information, PBE can encourage keyword look with complex questions over encoded information: Scenario III by the CSP; and in Scenario IV by an administration client. This utilization of PBE is fairly intriguing in that the concentration of these situations is on the CSP

and not benefit client, and is definitely deserving of further examination. The utilization of PBE Inside the cloud seems, by all accounts, to be aggregated at both the PaaS and SaaS benefit layers. In summation, the situations displayed in this study do demonstrate that the utilization of PBE in the Cloud is worthwhile.

REFERENCES:

D. Boneh and M. Franklin (2003). Identity-based encryption from the Weil pairing. SIAM Journal of Computing, 32(3): pp. 586–615.

D. Catteddu and G. Hogben (2009). Cloud computing: benefits, risks and recommendations for information security. Technical report, European Network and Information Security Agency.

D.A. Menascé and P. Ngo (2009). Understanding cloud computing: Experimentation and capacity planning. In Computer Measurement Group Conference.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In: STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing. pp. 169–178.

Jonathan Katz, Amit Sahai, and Brent Waters (2008). Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology, EUROCRYPT'08.

M. Barbosa and P. Farshim (2011). Delegatable homomorphic encryption with applications to secure outsourcing of computation. Cryptology ePrint Archive, Report2011/215.

N. Santos, K.P. Gummadi, and R. Rodrigues (2009). Towards trusted cloud computing. In Proceedings of the 2009 conference on Hot topics in cloud computing, page 3. USENIX Association.

S. Benabbas, R. Gennaro, and Y. Vahlis (2011). Verifiable delegation of computation over large datasets. In Proceedings of CRYPTO.

V. Goyal, O. Pandey, A. Sahai, and B. Waters (2006). Attribute-based encryption for fine- grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security (CCS).

Wang, S., Agrawal, D., El Abbadi, A. (2011). A comprehensive framework for secure query processing on relational data in the cloud. In: Proceedings of the 8th VLDB international conference on Secure data management. SDM'11 pp. 52–69.

Corresponding Author

Abhijit Trimbak Parchure*

Ph.D. Research Student, MUIT, Lucknow

E-Mail – abhijitparchure@yahoo.com