International Journal of Science Technology and Management
Vol. No.4, Issue 07, July 2015
www.ijstm.com
ISSN 2394 - 1537

KEYWORD BASED SEARCH OVER OUTSOURCED ENCRYPTED DATA USING VERIFIABLE ATTRIBUTE BASED

D.Bala Gurappa [1], B Dada Khalande[2], G. Rama Subba Reddy[3]

[1]M.tech Scholar (CSE), [2]Asst.Professor, Dept. of CSE, Vignana Bharathi Institute of Technology (VBIT),Vidya Nagar,Pallvolu, Proddatur,Kadapa(Dist),Andhra Pradesh (India)

[3]Working as Associate Professor and Head of Department (CSE),

Vignana Bharathi Institute of Technology (VBIT), Vidya Nagar, Pallvolu, Proddatur, Kadapa (Dist), Andhra Pradesh (India)

ABSTRACT

Search over encrypted data is a critically important enabling technique in Cloud computing, where encryption-before outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment. Many secure search schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, i.e. multi-user multi-contributor case. Inspired by verifiable attribute-based encryption (VABE), we present the first verifiable attribute-based keyword search scheme with efficient user revocation (VABKS-UR) that enables scalable fine-grained (i.e. File-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file. Further, by incorporating proxy re-encryption and lazy re-encryption techniques, we are able to delegate heavy system update workload during user revocation to the resourceful semi-trusted cloud server. We formalize the security definition and prove the proposed VABKS-UR scheme selectively secure against chosen-keyword attack.

I. INTRODUCTION

Internet technology is growing quickly, and people can process, store, or share with their data by using its ability. Recently, the cloud has emerged to provide various application services to satisfy user's requirement. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques. Cloud computing allows data owners to use massive data storage and vast computation capabilities at a very low price. Despite the benefits, data outsourcing deprives data owners of direct control over their outsourced data. To alleviate concerns, data owners should encrypt their data before outsourcing to the cloud. However, encryption can hinder some useful functions such as searching over the outsourced encrypted data while enforcing an access

ISSN 2394 - 1537

control policy. Moreover, it is natural to outsource the search operations to the cloud, while keeping the outsourced data private.

One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a cipher text grows with the complexity of the access policy. This primitive allows a data owner to control the search, and use of, its outsourced encrypted data according to an access control policy, while allowing the legitimate data users to outsource the (often costly) search operations to the cloud and verify whether or not the cloud has faithfully executed the search operations. In other words, a data user with proper credentials (corresponding to a data owner's access control policy) can (i) search over the data owner's outsourced encrypted data, (ii) outsource the search operations to the cloud, and (iii) verify whether or not the cloud has faithfully executed the search operations. We formally define the security properties of VABKS and present a scheme that provably satisfies them. The scheme is constructed in a modular fashion, by using attribute-based encryption, bloom filter, digital signature, and a new building-block we call attribute-based keyword search (ABKS) that may be of independent value. Experimental evaluation shows that the VABKS solutions are practical.

II. RELATED WORK

In this subsection, we review some closely related works, to the best of our knowledge, no existing solution is adequate for what we want to achieve. In what follows we briefly review the relevant techniques.

Noninteractive Verifiable Computation:- Noninteractive verifiable computation enables a computationally weak client to outsource the computation of a function to one or more workers. The workers return the result of the function evaluation as well as a no interactive proof that the computation of the function was carried out correctly. Since these schemes deal with outsourcing of general computation problems and preserve the privacy of input data; they can be used to outsource decryption in ABE systems.

Attribute-Based Encryption (ABE):- Basically, this technique allows entities with proper credentials to decrypt a cipher text that was encrypted according to an access control policy [1]. ABE is a popular method for enforcing access control policies via cryptographic means. Depending on how the access control policy is enforced, there are two variants: KP-ABE (key-policy ABE) where the decryption key is associated to the access control policy [2] and CP-ABE (cipher text-policy ABE) where the cipher text is associated to the access control policy [3]. ABE has been enriched with various features (e.g., [4]). In this paper, we use ABE to construct a new primitive called attribute-based keyword search (ABKS), by which keywords are encrypted according to an access control policy and data users with proper cryptographic credentials can generate tokens that can be used to search over the outsourced encrypted data. This effectively prevents a data owner from knowing the keywords a data user is searching for, while requiring no interactions between the data users and the data owners/trusted authorities. This is in contrast to [5], where the data users interact with the data owners/trusted authorities to obtain search tokens.

Keyword Search over Encrypted Data:- The Keyword search over Encrypted data used to search over the data. Mainly, this technique allows a data owner to generate some tokens that can be used by a data user to search over the data owner's encrypted data. Existing solutions for keyword search over encrypted data can be classified into two categories: searchable encryption in the symmetric-key setting and searchable encryption in

ISSN 2394 - 1537

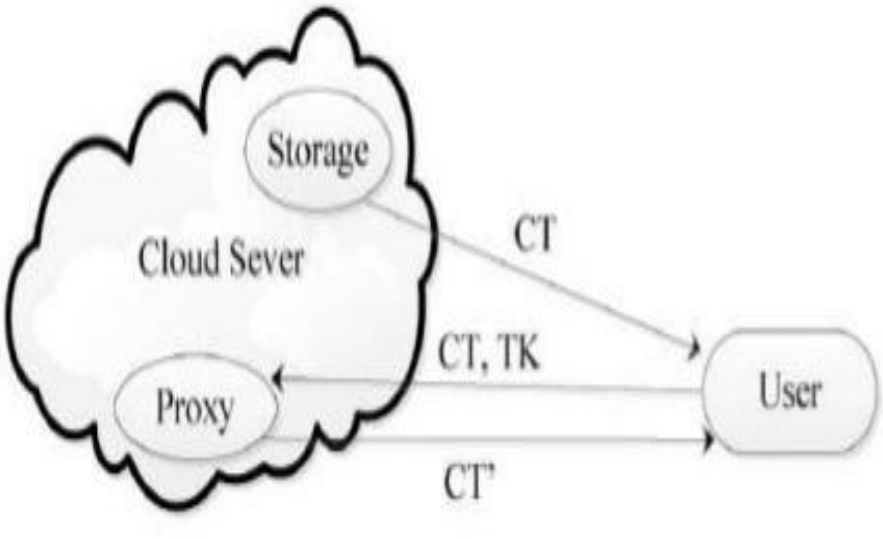
the public-key setting. Several variants have been proposed to support complex search operations. Moreover, searchable encryption in the multi-users setting has been investigated as well, where the data owner can enforce an access control policy by distributing some (stateful) secret keys to the authorized users. However, all these solutions do not solve the problem we study, because (i) some of these solutions require interactions between the data users and the data owners (or a trusted proxy, such as a trapdoor generation entity [2]) to grant search capabilities, and (ii) all these solutions assume that the server faithfully executed search operations. In contrast, our solution allows a data user with proper credentials to issue search tokens by which the cloud can perform keyword search operations on behalf of the user, without requiring any interaction with the data owner. Moreover, the data user can verify whether or not the cloud has faithfully executed the keyword search operations. This is true even for the powerful technique called predicate encryption which does not offer the desired verifiability.

Verifiable Keyword Search:-Recently, verifiable keyword search solutions have been proposed in, where each keyword is represented as a root of some polynomial. It is possible to check whether a keyword is present by evaluating the polynomial on the keyword and verifying whether the output is zero or not. However, these approaches work only when keywords are sent in plaintext to the cloud, and are not suitable for our purpose because the cloud should not learn anything about the keywords. It is worth mentioning that the secure verifiable keyword search in the symmetric-key setting [3] can be insecure in the public-key setting because the attacker can infer keywords in question via an off-line keyword guessing attack (in lieu of the off-line dictionary attack against passwords).

Paper Organization:- Section II reviews some cryptographic preliminaries. Section III defines VABKS and its security properties, presents KP-ABKS and CP-ABKS schemes and analyzes their security properties. Section IV defines VABKS and its security properties, presents the VABKS construction and analyzes its security. Section V evaluates the performance of the ABKS and VABKS schemes. Section VI concludes the paper.

Verifiable Attribute-Based Keyword Search:- In the model of ABKS, the party (e.g., cloud) is assumed to execute the search operation faithfully (despite that the party may attempt to infer useful information about the keywords). VABKS achieves the goal of ABKS despite that the party executing the search operation may be malicious.

We consider the system model illustrated in Figure 1, which involves four parties: a data owner, who outsources its encrypted data as well as encrypted keyword-index to the cloud; a cloud, which provides storage services and can conduct keyword search operations on behalf of the data users; a data user, who is to retrieve the data owner's encrypted data according to some keyword (i.e., keyword search); a trusted authority, which issues credentials to the data owners/users. The credentials are sent over authenticated private channels (which can be achieved through another layer of mechanisms).



The data owners are naturally trusted. Both authorized and unauthorized data users are semi-trusted, meaning that they may try to infer some sensitive information of interest. The cloud is not trusted as it may manipulate the search operations, which already implies that the cloud may manipulate the outsourced encrypted data.

III. CONCLUSION

In this paper, we considered a new requirement of VABE with outsourced decryption: verifiability. We modified the original model of VABE with outsourced decryption proposed by Green et al. [4] to include verifiability. We also proposed a concrete VABE scheme with verifiable outsourced decryption and proved that it is secure and verifiable. Our scheme does not rely on random oracles. To assess the practicability of our scheme, we implemented it and conducted experiments in a simulated outsourcing environment. As expected, the scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.

REFERENCES

[1] E.-J. Goh, "Secure indexes." Cryptology ePrint Archive, Report 2003/216, 2003. http://eprint.iacr.org/2003/216/.

[2] M. Chase, "Multi-authority attribute based encryption," in Proc. of TCC, pp. 515–534, 2007.

[3] F. Bao, R. H. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in Proc. of ISPEC, pp. 71–85, 2008.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS, pp. 89–98, 2006.

[5] D.X.Song, D. Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, pp. 44–, 2000.

International Journal of Science Technology and Management
Vol. No.4, Issue 07, July 2015
www.ijstm.com
ISSN 2394 - 1537

AUTHOR DETAILS

	***D.Bala Gurappa*** *pursuing M.Tech (CSE) Vignana Bharathi Institute of Technology (VBIT), VidyaNagar, Pallvolu, Proddatur, Kadapa(dist), Andhra Pradesh 516 362*
	***B Dada Khalander*** *received his M.C.A (Computer Science &Engineering) presently he is working as Assistant Professor in Vignana Bharathi Institute of Technology, Proddutur, Kadapa Dist. A.P, INDIA*
	***G.RamaSubbaReddy*** *received his M.E (Computer Science &Engineering) from Sathyabama University, Chennai.Presently he is working as Associate Professor and Head of the Department in Computer Science & Engineering, Vignana Bharathi Institute of Technology, Proddatur, KadapaDist.,A.P, INDIA*