ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Information Detection in Distributed Environment using Agents

S.Jhansi Rani, S.Rubini, K.Ravikumar

Post Graduate Student, Department of CSE, Rrase College of Engineering, Chennai, India.

Assistant Professor, Department of CSE, Rrase College of Engineering Chennai, India.

Professor, Department of CSE, Rrase College of Engineering, Chennai, India.

ABSTRACT - Data leakage is a budding security threat to organizations, particularly when data leakage is carried out by trusted agents. Using unobtrusive techniques for detecting data .Cloud is the main source for the owners to outsource the data. The data being outsourced to the cloud must be encrypted since the cloud is not trustful. There arises a range of problems, such as granting search capabilities to the data users by the owner, authorization for the data users search over a data owner's out sourced encrypted data, assurance that the cloud is faithfully to execute the search operations on their behalf. Verifiable attribute based keyword search (VABKS) is proposed to overcome the above problems. The solution allows a data user , whose credentials satisfy a data owner' s access control policy to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations.

KEYWORDS: Data leakage, encryption, agents, Attribute-Based Encryption, Keyword Search over Encrypted Data

I. INTRODUCTION

A data distributor has given sensitive data to a set of supposedly trusted agents (third parties). Sometimes sensitive data must be handed over to supposedly trusted third parties. For example, a hospital have maintain massive record and may give patient records to researchers who will devise new treatments with the help cloud, Cloud computing allows data owners to use massive data storage and vast computation capabilities at a very low price. Despite the benefits, data outsourcing deprive data owners of direct control over their outsourced data. To improve concern, data owners should encrypt their data before outsourcing to the cloud. However, encryption can hold back some useful functions such as searching over the outsourced encrypted data while enforcing an access control policy. Moreover, it is natural to outsource the search operations to the cloud, while keeping the outsourced data private. There is a need to allow the data users to verify whether the cloud faithfully executed the search operations or not and to detect the leakage of distributor's sensitive data by agents, and if possible to identify the agent that leaked the data and to propose data allocation strategies across the agent that improves the probability of identifying leakages. To the best of our knowledge, existing solutions cannot achieve these objectives simultaneously. This paper focuses on verifiable attribute-based keyword search (VABKS) to achieve the drawbacks of existing problem .

II. RELATED WORK

When the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data and for encrypting the data is achieved by follow these follows these relevant techniques, Attribute-Based Encryption (ABE) is a popular method for enforcing access control policies via cryptographic means. Basically, this technique allows entities with proper credentials to decrypt a cipher text that was encrypted according to an access control policy. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

owners/trusted authorities. Keyword Search over Encrypted Data 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.

III. PROPOSED ALGORITHM

A novel cryptographic solution is called verifiable attribute-based keyword search. This solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VABKS and describe a construction that satisfies them. A trusted authority, which issues credentials to the data owners/users. 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. Using 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 the keywords a data user is searching for, while requiring no interactions between the data users and the data owners/trusted authorities. In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. Decryption is the reverse process to encryption. Frequently, the same Cipher is used for both encryption and decryption. While encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. The algorithm is given below

1) Cryptographic Assumption:

Let p → ℓ-bit prime and G,GT → cyclic groups of prime order p with generators g, gT

e: G × G → GT satisfying these conditions, (where e → bilinear map)

i) for all a, b ← Zp, e(ga, gb) = e(g, g)ab,

ii) e (g, g) ≠ 1, and

iii) e can be computed

A) Decisional Linear Assumption (DL):

Given (g, f, h, f^{r1},g^{r2}, Q) where g, f, h, Q ← G, r1, r2 ← Zp

The advantage is defined as

|Pr [A (g, f, h, f^{r1}, g^{r2}, $^{hr1+r2}$) = 1] −Pr [A (g, f, h, f^{r1}, g^{r2}, Q) = 1]|

B) Generic Bilinear Group:

e : G × G → GT where G = { ϕ 0(x)|x € Zp} and GT = { ϕ 1(x)|x € Zp}

C) Pseudorandom Generator

H : $\{0, 1\}^{\ell}$→ $\{0, 1\}^{m}$, ℓ < m

2) Bloom Filter for Membership Query:

BF ← BFGen({H′ $_1$, . . . , H′ $_k$}, {w1, . . . , wn}) where dataset S= {w_1, . . . , w_n} with {H′ $_1$, . . . , H′ $_k$}

{0, 1} ← BFVerify({H′ $_1$, . . . , H′ $_k$}, BF, w) where 1→if w € S, 0→ otherwise

3) Attribute-based keyword search(ABKS):

1. initializes the public parameter pm and generates a master key mk

(mk, pm) ← Setup(1^{ℓ})

2. sk ← KeyGen(mk, I_{KeyGen}) where sk→ credential output

3. cph ← Enc(w, I_{Enc})

4. tk ← TokenGen(sk, w) allows a data user to generate a search token tk according keyword w.

5. {0, 1} ← Search(cph, tk): returns 1 if

(i)F (I_{KeyGen}, I_{Enc}) = 1 and

(ii) Cipher text cph and token tk otherwise return 0

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

IV. PSEUDO CODE

VABKS - Verifiable Attribute Based Keyword Search
Assume the following,
Let FS = {F_1, . . . , Fn} be a set of data files
Let KGj ,1 ⩽ j ⩽ l, be a set of keywords
Let MP(w) be the set of identifiers identifying data files that contain keyword w.
Let MP = {MP(w)|w € $U^{l}_{i=1}$=KG_i and
Let D = (KG, MP, FS) denote keyword-index
Step 1: To initialize the system (mk, pm) ← Init(1^{ℓ})
Step 2: Calculate the credential output sk ← KeyGen(mk, I_{KeyGen})
Step 3: (Au, Index, D_{cph}) ← BuildIndex({I_{Enc}}$_l$, {I'_{Enc}}$_n$, D) where D_{cph}→data ciphertext ,
{I_{Enc}}$_l$→access control policies of l keyword group
{I'_{Enc}}$_n$→ access control policies of n data group
Step 4: Then generate a token tk ← TokenGen(sk, w)
Step 5: Perform search operation over encrypted index by using
(proof , rslt) ← SearchIndex(Au, Index, D_{cph} , tk)
Step 6: Verify the validity respect to search token of the data user,
{0, 1} ← Verify(sk, w, tk, rslt, proof)
Step 7: End.

V. SIMULATION RESULTS

The simulation studies involves the process of creating very secure data distribution by means of verifiable attribute-based keyword search and also used for avoid data leakage and secure data distribution over cloud computing by using encrypted data .VABKS algorithm effectively filters out a mass of data and gives security like data secrecy, Keyword secrecy, Verifiability. The scheme is constructed in a modular fashion, by using attribute-based encryption, bloom filter, digital signature, and a new building-block that call as attribute-based keyword search (ABKS) that may be of independent value. This coincides with the desire happens of the data leakage.

VI. CONCLUSION AND FUTURE WORK

The recreation studies involves the primitive process called verifiable attribute-based keyword search for detecting data leakage and secure data distribution over cloud computing by using encrypted data. This prehistoric allows a data owner to control the search of its outsourced encrypted data according to an access control policy, while the certified data users can outsource the search operations to the cloud and force the cloud to faithfully execute the search (as a cheating cloud can be held accountable). Hence sharing of data should proceed by considering assumptions specified and may reduce the leakage through our efficient algorithm and by the process of Verifiable Attribute Based Keyword Search encryption algorithm. As such, one appealing open problem for potential delve into accommodate dynamic data.

REFERENCES

1. J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. of IEEE S&P, pp. 321–334, 2007.
2. J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorized private searches on public key encrypted data," in Proc. of PKC, pp. 196–214, 2009.
3. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of, pp. 79–88, 2006
4. Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Proc. of ICC, pp. 917–922, 2012
5. J. Katz and Y. Lindell, Introduction to Modern Cryptography. Chapman and Hall/CRC Press, 2007
6. R. Canetti, S. Halevi, and J. Katz, "Chosen-cipher text security from identity -based encryption," in EUROCRYPT, pp. 207–222,2004.
7. E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in Proc. Of TCC, pp. 457–473, 2009..

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

8. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in Proc. of ICDCS, pp. 383–392, 2011
9. 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..
10. T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," in Proc. of ASIACRYPT, pp. 214–231, 2009

BIOGRAPHY

Jhansi rani is a post graduate student in the department of computer science engineering, Rrase College of engineering, Anna University. She received Bachelor of Engineering degree (B.E) in 2010 from RMK engineering college, Anna University, Chennai, India. Her research interests are networking, cloud computing , Information Security etc.