ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 95- 99 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp19.pdf

Searching on Cloud Data by Using Secure Key Exchange System

M.Mounika[1], A.Ganesh[2]
[1]M.Tech, Dept of CSE, S.V. College of Engineering, Tirupati, AP, India
mounika.mukkara@gmail.com
[2]Assistant Professor, Dept of CSE, S.V. College of Engineering, Tirupati, AP, India,
achari.ganesh@gmail.com

ABSTRACT

Most basically, we determine and fix the tough problem of privacy-preserving multi-keyword rated look for over secured information in reasoning processing (MRSE). We set up a set of tight comfort specifications for such a protected reasoning information usage system. Among different varieties of multi-keyword semantics, we prefer the effective likeness assess of "coordinate related," i.e., as many suits as likely, to catch the importance of information records to the look for question. We additionally use "inner item similarity" to quantitatively assess such likeness assess. We initially recommend an essence for the MRSE based on protected internal item calculations, and then give two radically enhanced MRSE techniques to attain various tight comfort specifications in two unlike risk models. To improve look for experience of the information look for service, we further increase these two techniques to support more look for semantics. Thorough research analyzing comfort and performance assures of suggested techniques is given. By performing the test on the real world information set proves that suggested techniques are certainly low expense on calculations and interactions Here we propose agreement called Password – authenticated key (PAKE) in which client and server share a secret password by confirming with each other and provide cryptographic key for trade of data. Incase if server is attacked due to professional attacks, passwords in the server will be exposed. So in this thesis, we believe of using two servers to check the client when one server is failed. So that the opponent cannot get the data from affected server by acting like client. Present result for two server PAKE are either utilize two servers equally for verification or one server with the help of another server checks the client. Here we provide a balanced result for two server PAKE, where consumer can set dissimilar keys with two severs. This protocol is effective when compared to present protocol in requisites of similar calculations.

1.INTRODUCTION

CLOUD computing is dreamed service, where clients can accumulate their data into the cloud so to have the benefit of the efficient services from a portable of resources with greater flexibility and economic savings. To defend data confidentiality and contest spontaneous accesses in the cloud for example, e-mails, photo albums, financial transactions, and so on.

The data owner encrypt the data before outsourcing to the open cloud but downloading and decrypting the data locally is totally unreasonable data, due to large quantity of bandwidth cost.. Thus, considering solitude-conserving and efficient search service over encrypted cloud data is of vital significance. In view of Potentiality, great number of recommended data users and vast sum of redistribute data credentials in the cloud and it will be particularly challenging to meet the requirements of performance, system usability, and scalability. As there is need for effective data retrieval we use ranked search service system to collect relevant data by avoiding unwanted network traffic and provides privacy protection there by provides accuracy to boost the individual browsing skill. it is essential for grade system to supports multiple keywords search. e.g.: Google search

"Coordinate matching" has been extensively used in the plaintext information retrieval (IR) community. To apply in the cloud data system is a tough task because of inbuilt defense and solitude obstacle.

2. SYSTEM ARCHITECTURE

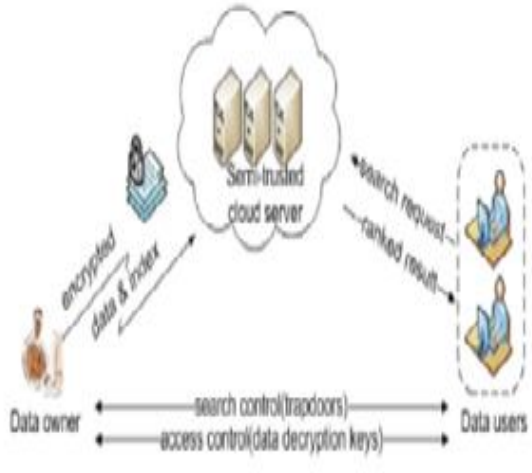

Figure 1: Architectural Model

The cloud service involves three different components, as shown in the above architecture; the data owner, the data user, and the cloud server. The data owner has a set of record papers F that can be stored in the cloud server in the

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 95- 99 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp19.pdf

encrypted form C by enabling search for efficient source utilization .it first builds the index I for search purpose then it stores I and F in cloud server. To explore the document collection for t given keywords, an certified customer obtain a corresponding trapdoor T through search control technique, for example, broadcast encryption. By getting T from data user, the cloud server will be in charge to search index I and send back the related files .To progress the data retrieval accuracy, we use grading criteria. Additionally, to lessen the message cost, the cloud server only sends back top-k documents that are most significant to the search query when data user sends optional number K along with the trapdoor T.Lastly, the access control method is engaged to supervise the insertion, deletion, updation of documents.

Advanced research in password-based authentication has permitted a user and a server jointly to validate a password and for secure communications we use cryptographic key following validation. In broad-spectrum, present solutions for password based verification follow two models. The former model, called PKI-based model, assumes that the user will have public key of the server along with the password to share with the server; Here client will send the password by using key. The succeeding model is known as password-only model. In "encrypted key exchange" protocols, for encrypt numbers we use the password as secret key that is used exchange purpose. In identity based model, server stores the password along with the private key. Incase if client forgets the password it can be provided by server which should be encrypted by client. This representation is between the password only models and the PKI-based. The distinctive protocols for password-based verification imagine a particular server stores all the passwords required to validate users. If the server is affected, due to hacking, the passwords stored in server will be exposed. In this thesis, we put forward a new balanced solution for two-server PAKE. In which two servers share passwords i.e. pw1 and pw2 are subjected to pw1+pw2=pw.

3. SOLITUDE REQUIREMENTS FOR MRSE

By providing the privacy assurance in the allied writing in which server should not check the details but just provide the search results. With this explanation, we discover and create a specified set of solitude requirements for the MRSE framework. As for the data privacy, the data owner should encrypt the data by using cryptography before outsourcing and effectively preventing cloud to snoop the data that is provided by the data owner. Incase of index privacy, if the cloud deduce any relation between documents and keywords. There may be a chance of learning small amount of document so we should construct a searchable index with which cloud can provide the results without prying of content. The index and data privacy are generally demanded as a customary in literature. The confidential requirements involved in query process is more difficult to manage such as Keyword privacy. The clients don't like to disclose their searches to others i.e. cloud and it is important for them to conceal what they are searching. By using trapdoor to guard which is generated by cryptographic method for query keywords. The cloud can estimate the results by using statistical analysis by document frequency is enough to show the keyword with elevated range. When the cloud have backdrop data of data set. We can use this explicit data to reverse engineer the keyword. Trapdoor: unlink-ability. The trapdoor generation function should be a arbitrary way instead of ritualistic. So, the server should not realize the relationship between trapdoors, for example, If two trapdoor are formed ritualistic method then cloud will gather the frequencies of diverse request of unlike keywords which violates requirements of privacy. So we should introduce trapdoors: unlink-ability to stop ritualistic generation method.

4.SOLITUDE-CONSERVINGAND COHERENT MRSE

To professionally accomplish multi-keyword ranked search, we intend to utilize "inner product similarity" to quantitatively assess the competent resemblance assess "coordinate matching." exclusively, D is a binary data we initially recommend a vital plan for the MRSE using secure inner product calculation, which is personalized from a secure kNN technique, and then show considerably develop the solitude-conserving against diverse threat models in the MRSE framework in a bit by bit procedure. We also discuss supporting more search semantics and dynamic operation.

4.1 MRSE_I: Solitude-Conserving Design in Known Cipher text Model:

The modified locked internal artifact calculation format will not be sufficient for our MRSE design. The foremost reason is arbitrary involved is the scale factor r in the trapdoor generation that the only randomness implicated is the scale factor r in the trapdoor generation, which does not provide enough assurance required by trapdoor and keyword privacy requirement. To develop a more sophisticated design for the MRSE ,we offer MRSE_I scheme.

4.1.1 MRSE_I Scheme

In this highly developed plan, as a substitute of removing the complete measurement present in the query vector as we decided to do at former peek, we protect this measurement procedure but provide a new arbitrary number t to measurement in each query vector. By adding randomness enhance the complexity for cloud to discover about link between the trapdoors. As mentioned before randomness should be calibrated carefully to obscure the search result for DF and reduce the probability for re-discovery of keywords. By providing some randomness in the last rendering achieve is an successful way. More exclusively, unlike the randomness in query vector, we include a fake keyword into each data vector and allot a casual value to it.
Each individual vector D is extended to þ 2Þ-dimension instead of þ 1Þ, where a casual variable "Representing the dummy keyword is stored in the extended dimension. The

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 95- 99 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp19.pdf

whole scheme to achieve ranked search with multiple keywords over encrypted data is as follows:

$$l_i \,.\, T_W^- = \{M_1^T\, D_1' \,.\, M_2^T\, D_1^{"}\} \,.\, \{M_1^{-1}\, Q^1 \,.\, M_2^{-1}\, Q^{"}\}$$
$$= D_1' \,.\, Q' + D_1^{"} \,.\, Q^{"}$$
$$= D_i \,.\, Q$$
$$= (D_i \,.\, c_i \,.1) \,.\, (rQ \,.\, r.t).$$
$$= r(D_i \,.\, Q + c_i) + t$$

4.2 MRSE_I_TF

In the grading set "coordinate matching," the occurrence of keyword in the manuscript or the question is shown as one in the data or query vector. Actually, there are more number of components that could make collision on the search usability. For example, when 1 keyword appears in most documents present in the data set, the significance of this keyword in the question will be less than other keywords which appears in fewer document. Similarly, if query keyword is present in multiple locations of one document then client prefers the document which contain question keyword in single position. To confine these data in the search process, we use the TF _ IDF weighting rule within the vector space model to estimate the likeness, where TF is term frequency and IDF is document frequency. Amid of some hundred variations of the TF _ IDF weighting scheme, no single mixture of them out performs any of the others collectively. Thus, without failure of synopsis, here we select an instance rule that is usually used and broadly seen in the literature

$$Score(F_i,Q) = \frac{1}{|F_1|} \sum\nolimits_{-} (1 + \ln f_{i,j}) \,.\, \ln\left(1 + \frac{m}{f_j}\right) \qquad (4)$$

$\ln(1 + \frac{m}{f_j})$, Finally,the similarity score is as follows:

$$I_i \,.\, T_W^- = r(D_i \,.\, Q + c_i) + t$$
$$= r\left(\sum_{w_j \varepsilon Q} \frac{1+\ln f_{i,j}}{|F_i|} \,.\, \ln 1 + \frac{m}{f_j} + c_i\right) + t \qquad (5)$$
$$= r(Score(F_i,Q) + c_i) + t$$

Therefore, the likeness of the manuscript and the question in conditions of cosine angle between the document and the query vector could be assessed by calculating the internal product of sub index I and trapdoor.Even though this comparison dimension introduces more calculation price during the index creation and trapdoor generation, it records more allied data on the content of manuscript and question for better results of clients' concern.

4.3 MRSE_II_TF

Here, even though some records present in D have been altered from binary value 1 to normalize term regularity, the level study assault still partly works in the known backdrop model. With like situation in the prior section, the former question contains two keywords as

$$y_{1=r\left(\frac{1+\ln f_{1,1}}{|F_1|} \ln(1 + \frac{m}{f_1}\right) + \frac{1+\ln f_{1,2}}{|f_1|} .\ln(1 + \frac{m}{f_2}\right) + c_1) + t;$$
$$y_{2=r\left(\frac{1+\ln f_{2,1}}{|F_2|} \ln(1 + \frac{m}{f_1}\right) + c_2) + t;$$
$$y_3 = rc_3 + t;$$
$$y'_{1=r'\left(\frac{1+\ln f_{1,1}}{|F_1|} \ln(1 + \frac{m}{f_1}\right) + \frac{1+\ln f_{1,2}}{|f_1|} .\ln(1 + \frac{m}{f_2}\right) + c_1) + t';$$
$$y'_{2=r'\left(\frac{1+\ln f_{2,1}}{|F_2|} \ln(1 + \frac{m}{f_1}\right) + c_2) + t'$$
$$y'_3 = r'c_3 + t';$$

4.4 D-H Key Exchange Protocol

In 1976 Diffie and Hellman invented a protocol called Diffie-Hellman key exchange protocol. It was the former rational method which is used by the users to share secret key created over an insecure communication channel. Even though it is a invalid key exchange protocol, it provides the foundation for a range of genuine protocols.RSA is shortly followed by the Diffie-Hellman key exchange protocol. Consider two users A and B, who doesn't have any information about each other but desire to set up a locked connection between them, by using D-H key exchange protocol.

5 . PASSWORD AUTHENTICATION BY TWO-SERVER AND EXCHANGE OF KEY

5.1 Model

In our structure, we have two server S_1 , S_2 and a cluster of clients. The two servers oblige with each other to legalize the users and offer favour to valid users former to verification, every client C chooses a password pw

And $Auth_C^{(2)}$ for S_1 and S_2 respectively, such that nobody Can determine the password pw_C and $Auth_C^{(1)}$ *or* $Auth_C^{(2)}$ *Unless* S_1 and S_2 respective, through dissimilar protected Channels during the customer registration.

Once that the user solutions for two-server PAKE, we believe that the two servers never plan to disclose the client password. When the servers oblige to certify a client C, we can think that the client C can transmit a message to both of S_1 and S_2 concurrently, but we should not presume a advertise channel in particular because an enemy can convey a different message to the servers or refuse to convey. In this technique, the client and server communicates through a open channel which can be intrude, delayed, rephrase and even meddled by an enemy.

Our procedure is a balanced, if two servers equally donate to authenticate in terms of calculation and conveyance. An opposition in our structure is either submissive or dynamic. We believe both online vocabulary attacks and offline

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 95- 99 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp19.pdf

vocabulary attacks, In former an invader tries to sign-in frequently In latter an opposition derives information about the password from practical transcripts of record sessions. By using cryptographic method we cannot prohibit the online attack but can be easily diagnose and suspend once the validation fails numerous times.

We believe that an rival can negotiation one server only and collect all data stocked in the server. The communication between the client and two server can be controlled by a submissive rival. A dynamic rival will pretend that communication process is between genuine client and server but deviate in a random way from the events described by the procedure. In our procedure, A secret session key recognized between the client and the sincere server which will be attempted by the rival to learn about it. In an dynamic attack, if rival is determined to learn the secret password from the client and server then it will be possible only if rival know client password. In common, we say that our procedure is safe if no foe can be successful in any submissive and dynamic attacks in case that one server is mutual concession. Hence it defines about the foe succeeds in a submissive attack or a dynamic attack.

5.2 Validation and Exchange of Key

Presume that the two servers S_1 and S_2 have received the password authentication data of a client C during the registration, Here it will five steps for the two servers S_1 and S_2 to validate the client C and launch secret session keys with the client C in terms of corresponding calculation.

Step 1: The client *C* randomly chooses an integer r from $И_q^*$,computes R=$g_1^r g_2^{-pw_c}$ and then broadcasts a Request message M_1={C,Req,R} to the two server S_1 and S_2.

Step 2:On receiving M_1,the server S_1 randomly chooses An integer $r_1$from $И_q^*$ and computes

$$A_2' = A_2^{r_1},$$
$$B_2' = (R.B_2)^{r_1}$$

The server S_2 randomly chooses an integer r_2 from $И_q^*$ and computes

$$A_1' = A_1^{r_2},$$
$$B_1' = (R.B_1)^{r_2}$$

Then S_1 and S_2 exchange $M_2 = (A_2', B_2')$ *and* $M_3 = (A_1', B_1')$.

Step 3:On receiving $(A_1', B_1')$the server S_1 randomly chooses An integer $r_1'$from $И_q^*$ and computes

$$R_1 = A_1'^{a_1^{-1} r'_1}$$

$$K_1 = (B_1' / A_1'^{x}) r_1'$$

$$h_1 = H(K_1, 0) \oplus b_1$$

And replies $M_4 = (S_1, R_1, h_1)$to the client C

On receiving $(A_2', B_2')$the server S_2 randomly chooses An integer $r_2'$from $И_q^*$ and computes

$$R_2 = A_2'^{a_2^{-1} r'_2}$$
$$K_2 = (B_2' / A_2'^{x}) r_2'$$

$$h_1 = H(K_2, 0) \oplus b_2$$

And replies $M_5 = (S_2, R_2, h_2)$to the client C

Step 4:After receiving M_4 *and* M_5, the client C computes

$$K_1' = R_1^r, K_2' = R_2^r,$$

And checks if

$$H(K_1',0) \oplus H(K_2',0) \oplus h_1 \oplus h_2 = H(pw_c)$$

If so,the two servers S_1 and S_2 are authentic The Client C computes

$$h_1' = H(K_1', 1) \oplus H(K_1', 0) \oplus h_1$$

$$h_2' = H(K_2', 1) \oplus H(K_2', 0) \oplus h_2$$

And then broadcasts.$M_6 = \{h_1', h_2'\}$At last,the client C Sets the secret session keys with S_1 and S_2 as $SK_1' = H(K_1', 2)$ *and* $SK_2' = H(K_2', 2)$, Respectively.

6. PROTECTION OF OUR PROTOCOL

Here, we will present safety evidence of our protocol against the inactive assault and the dynamic assault, respectively.

6.1 Protection Against Submissive Assault

Since our protocol is balanced, we have to believe that inactive assault, where A as inactive rival sho uld have mutual concession for the server S_2 which also able to play the role of monitor and all interactions between S and C attempts to learn the secret session key which is established between them.Instead key exchange authentication is done by hash function. To shorten the safety analysis, ignore the message of hash values in our procedure. Like [3], [19], [20], [21], we define the security of our procedure with the help of a game,where after establishing a secret session key K 1 Þ, the rival A is provided with either K Þ or an casual element in

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 95- 99 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp19.pdf

GG with equally probability to guess.If A can guess correctly then A can win the game.

6.2 Performance Analysis

Participants	YDB Protocol	JWX Protocol	Our Protocol
Client C	Comm. $4L+2l$ Comp 5 Rounds 6	Comm. $6L+2l$ Comp 6 Rounds 3	Comm. $3L+4l$ Comp 4 Rounds 3
Server S_1 (SS)	Comm. $8L+3l$ Comp 6 Rounds 10	Comm. $11L+3l$ Comp 8 Rounds 6	Comm. $6L+3l$ Comp 5 Rounds 4
Server S_2 (CS)	Comm. $4L+1l$ Comp 3 Rounds 4	Comm. $5L+1l$ Comp 4 Rounds 3	Comm. $6L+3l$ Comp 5 Rounds 4
Total Running Time (Server Side)	Comm. $8L+3l$ Comp 9 Rounds 10	Comm. $11L+3l$ Comp 12 Rounds 6	Comm. $6L+3l$ Comp 5 Rounds 4

TABLE : Contrast of Performance between Our Protocol ,YDB and JWX Protocols

7.CONCLUSION

In this thesis, we have offered a balanced procedure for password authentication by two-server and key exchange.

If one among the two servers is compromised, Security analysis shows that our protocol is safe against submissive and dynamic attacks. Performance study has revealed that our protocol is more capable when compared to the other two server PAKE protocols.

REFERENCES

[1] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.

[2] M. Abdalla, O. Chevassut, and D. Pointcheval, "One-Time Verifier-Based Encrypted Key Exchange," Proc. Eighth Int'l Conf. Theory and Practice in Public Key Cryptography (PKC '05), pp. 47-64,2005.

[3] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 139-155, 2000.

[4] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password Based Protocol Secure against Dictionary Attack," Proc. IEEE Symp. Research in Security and Privacy, pp. 72-84, 1992.

[5] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01), pp. 213-229, 2001.

[6] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.

[7] D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp., pp. 241-250, 1998.

[8] V. Boyko, P. Mackenzie, and S. Patel, "Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.

[9] J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New TwoServer Approach for Authentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.

[10] W. Diffie and M.E. Hellman, "New Directions in Cryptography,"IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654,Nov. 1976.

[11] M. Di Raimondo and R. Gennaro, "Provably Secure Threshold Password Authenticated Key Exchange," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '03), pp. 507-523, 2003.

[12] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[13] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 176-180, 2000.

[14] O. Goldreich and Y. Lindell, "Session-Key Generation using [21] J. Katz and M. Yung, "Scalable Protocols for Authenticated Group Key Exchange," Proc. Advances in Cryptology Conf. (Crypto '03)