FINE-GRAINED DUAL-FACTOR SECURITY MECHANISM FOR DATA DISTRIBUTION IN CLOUD STORAGE

[1]E.MANISHA, [2]MR.V.RAVIKUMAR VEMULA

[1] PG Student, Department of Computer Science and Engineering, Chaitanya institute of technology and science Kishanpura,Hanamkonda,Warangal -506001, (.TS).india

[2]Assistant Professor, Department of Computer Science and Engineering ,Chaitanya institute of technology and sciencekishanpura,Hanamkonda,Warangal -506001, (TS).india

[1]manishaenumula@gmail.com,[2]ravikumar.vemula@hotmail.com

Abstract:

Data sharing in cloud storage is receiving substantial attention in Information Communications Technology, since it can provide users with efficient and effective storage services. To protect the confidentiality of the shared sensitive data, the cryptographic techniques are usually applied. However, the data protection is still posing significant challenges in cloud storage for data sharing. Among them, how to protect and revoke the cryptographic key is the fundamental challenge. To tackle this, we propose a new data protection mechanism for cloud storage, which holds the following properties. 1) The cryptographic key is protected by the two factors. Only if one of the two factors works, the secrecy of the cryptographic key is held. 2) The cryptographic key can be revoked efficiently by integrating the proxy re-encryption and key separation techniques. 3) The data is protected in a fine-grained way by adopting the attribute based encryption technique. Furthermore, the security analysis and performance evaluation show that our proposal is secure and efficient, respectively.

.

I.INTRODUCTION

Social media has become a major source of information foranalyzing all aspects of daily life. In particular, Twitter isused for public health monitoring to extract early indicatorsof the well-being of populations in different geographicregions. Twitter has become a major source of data for earlymonitoring and prediction in areas such as health [1], disastermanagement [2] and politics [3]. In the health domain,the ability to model transitions for ailments and detectstatements like "people talk about smoking and cigarettesbefore talking about respiratory problems", or "people talkabout headaches and stomach ache in any order", benefits syndromic surveillance and helps measure behavioral riskfactors and trigger public health campaigns. In this paper,we formulate two problems: the health transition detectionproblem and the health transition prediction problem. To addressthe detection problem, we develop TM–ATAM that modelstemporal transitions of health-related topics. To address theprediction problem, we propose T–ATAM, a novel methodwhich uncovers latent ailment inside tweets by treatingtime as a random variable natively inside ATAM[4]. Treatingtime as a random variable is key to predicting the subtle changein health-related discourse on Twitter.

Common ailments are traditionally monitored by collectingdata from health-care facilities, a process knownas sentinel surveillance. Such resources limit surveillance,most especially for real-time feedback. For this reason, the Web has become a source of syndromic surveillance, operating on a wider scale, near real time and at virtually no cost. Our challenges are: (i) identify health-related tweets, (ii)determine when health-related discussions on Twitter transitionsfrom one topic to another, (iii) capture different such transitionsfor different geographic regions. Indeed, in addition to evolvingover time, ailment distributions also evolve in space.Our experiments on a corpus of more than 500K healthrelatedtweets collected over an 8-month period, show thatTM–ATAM outperforms TM–LDA in estimating temporaltopic transitions of different geographic populations. Ourresults can be classified in two kinds of transitions. Stabletopics are those where a health-related topic is mentionedcontinuously. One-Way transitions cover the case where sometopics are discussed after others. For example, our studyof tweets from California revealed many stable topics suchas headaches and migraines. On the other hand, tweetingabout smoking, drugs and cigarettes is followed by tweetingabout respiratory ailments. Figure 1 shows example onewaytransitions we extracted for different states and cities inthe world. Such transitions are often due to external factorssuch as climate, health campaigns, nutrition and lifestyle of different world populations.

II.EXISTING SYSTEM:

Cryptographic bit of leeway helping revocability is consciousness single re-encryption (PRE) which changed into proposed with the aid of Blaze et al. In an inside man or woman re-encryption plot, a boss (e.G., the semi-relied on in cloud) can alternate a ciphertext for a consumer into some other ciphertext that another consumer can unscramble while the cross-among can ace simply the duration of the ciphertext.

- PRE may be formalized into plans regarding the direction of advancement: bidirectional and unidirectional.
- In bidirectional PRE, the agent can trade the ciphertext from one client into every other client and the alternative manner. In unidirectional PRE, inside character can essentially trade a couple of way. To make the capacity and security of PRE, numerous plans had been proposed.

Disadvantages of Existing System:

We express that solidifying the ABE and PRE methodologies, the subsequent blueprint nevertheless can't fulfill appropriate necessities in the records sharing circumstance for handed on figuring.

•In express, it can't brace the 2-element protection

III.PROPOSED SYSTEM:

To realize the inadequacies of the dazed route of motion, we be a part of the pleasant based encryption framework, attention specific re-encryption structure, and the important thing region soundness to dissipate the usage of PKE and the cutoff of safety contraption's riddle within the key age center even as coordinating key presentation and disavowal issues and assisting fine-grained discover the risk to govern.

- In LLS+15, the ciphertexts are of tactics. One is the IBE ciphertext, the alternative is the PKE ciphertext. Regardless, all of the ciphertexts in our proposed framework are ABE ciphertexts. The great endeavors to make our shape work well are the course by means of which the antique protection contraption is repudiated and how the brand new safety tool can do loosening up sensibly.
- To revoke the old protection contraption, we want that the cloud continues the antique ciphertexts earlier than sending them to the customer with the aid of using pass among re-encryption framework. In reality while the client requests the new protection contraption, the client should supply an trouble to the key age middle to make some other solicitation which can be used to unscramble the reestablished ciphertexts.

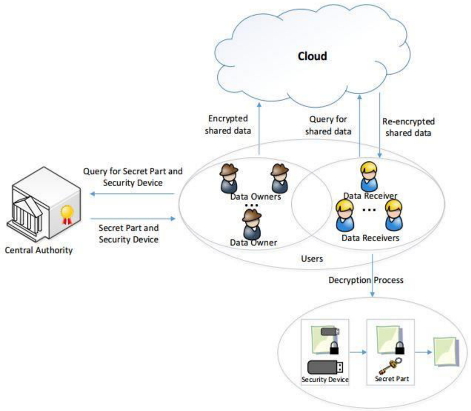
Advantages of Proposed System:

LLS+15 is in a standard sense related with for comfy facts confirming even as our preferred awareness is for cozy statistics sharing. Those are two hypnotizing functionalities given with the aid of distinctive forms of cryptographic outlines.

- We use a replacement approach to manipulate welcome the 2-component strategy to disentangle the key presentation and key renouncing issues. Along these strains, handiest a solitary type of ciphertexts exists in our solution, which makes our solution sensibly clean and execute. Moreover, the important thing age middle in our recommendation does now not want to keep a few different first rate bits of adjusting near its personal special non-public key.
- We unequivocally showcase that how the unscrambling is proceeded with out revealing the riddle set away in the safety contraption.
- at the same time as this part isn't always referenced in LLS+15.

While we use ABE as IBE, our proposition is greater suit than LLS+15 to the diploma computational cost and restriction value.

SYSTEM ARCHITECTURE:



IV.IMPLEMENATATION:

Central Authority:

In this module, the principal Authority is a relied on in get-collectively that is in price of issuing the cryptographic key for each patron as confirmed up via their great set and after that element it into portions (-element): One, known as as secret element Key (SPK), is perceived to be checked in a capability-mistaken spot (e.G., pc). The opposite, named as security device Key (SDK) is checked in a physically-relaxed regardless computationally obliged contraption (protection device). Basically, the CA is in like way accountable for reviving each purchaser's safety contraption (and the looking). Astoundingly, inside the SDK update kind out, the CA makes every other SDK this is licensed in a safety contraption and the pertaining to re-encryption key so that it will be sent to the cloud. Note that the re-encryption key's used to enable the ciphertexts to make the brand new SDK paintings, at the same time as the generationof the re-encryption key calls for the information of the old SDK. As referenced mid, one of the upsides of our idea is that the CA does not need to save any thrilling bits of statistics for clients. For this situation, the course by way of which that the CA for the most part problem an replace key to engage the old SDK can't paintings in attitude at the missing of the vintage SDK (the security contraption can be stolen or lost). To cope with the problem, we use SPK to get well SDK.

Cloud: In this module, the cloud is a semi-trust birthday celebration that shops all combined shared records and maintains up a desk Table containing the clients' in depth individual (UID) and pertaining to re-encryption key.

Proper while a Data Receivers (DR) power for the everyday data, the cloud goes about as a judge to re-scramble the encoded shared information by using DR's concerning re-encryption key and returns the re-combined shared data to information Receivers.

Records owners (Dos):

On this module, the information proprietor (DO) is a patron who needs to offer statistics to numerous customers (DRs). All the most facts are encoded by means of the usage of CP-ABE consistent with the manner framework.

Statistics Receivers (DRs)

A DR is a purchaser who can get the not unusual statistics from the cloud. Right while a DR wishes to recuperate the ordinary facts, the cloud from the outset does re-encryption and a quick time period later reestablishes the following re-encoded ciphertext. The reencryptedciphertext may be unscrambled by the use of DR's very very own ascent SPK and SDK, if DR's excellent set satisfies the way route of motion of the usual information. Word that SDK is never discovered out of the safety device in the midst of the unscrambling, whilst a midway unwinding approach the use of SDK could be achieved within the security contraption. Proper when the safety contraption is misplaced or stolen, DR can deny it and get some other safety tool via managing CA..

V.CONCLUSION:

In this paper, we proposed a fine-grained two-factor data protection for cloud storage. The two-factor is realized by separating the secret key into two parts, one can be stored in a potential-insecure place, and the other is stored in a tamper resistant device. Only if one of them is kept secret, the proposal remains secure. Furthermore, with the help of CPABE and PRE, we obtained the fine-grained access control on encrypted data and the revocability of tamper resistant device, respectively

VI.REFERENCES:

[1] "Pcloud," www.pcloud.com/.

[2] C.Wang, S. S. Chow, Q.Wang, K. Ren, andW. Lou, "Privacy-preservingpublic auditing for secure cloud storage," Computers, IEEE Transactionson, vol. 62, no. 2, pp. 362–375, 2013.

[3] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamicaudit services for outsourced storages in clouds," Services Computing,IEEE Transactions on, vol. 6, no. 2, pp. 227–238, 2013.

[4] H. C. Chen, Y. Hu, P. P. Lee, and Y. Tang, "Nccloud: a networkcoding-based storage system in a cloud-of-clouds," Computers, IEEETransactions on, vol. 63, no. 1, pp. 31–44, 2014.

[5] "Encryption key virus threat," http://searchsecurity.techtarget.com/tip/Encryption-key-virus-threat.

[6] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems,"in Advances in Cryptology–EUROCRYPT 2002. Springer,2002, pp. 65–82.

[7] B. Libert, J.-J. Quisquater, and M. Yung, "Parallel key-insulated publickey encryption without random oracles," in Public Key Cryptography–PKC 2007. Springer, 2007, pp. 298–314.

[8] A.-A. Ivan and Y. Dodis, "Proxy cryptography revisited." in NDSS, 2003.

[9] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertextsecureproxy re-encryption," in Public Key Cryptography–PKC 2008. Springer,2008, pp. 360–379.

[10] J. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-factor datasecurity protection mechanism for cloud storage system," Computers,IEEE Transactions on, vol. 65, no. 6, pp. 1992–2004, 2016.