**Result-Pattern Hiding Searchable Encryption for Conjunctive Queries**

(E.GANESHKUMAR)

(MASTER OF COMPUTER APPLICATIONS,

SRI PADMAVATHI COLLEGE OF COMPUTER

SCIENCES AND TECHNOLOGY TIRUCHANOOR,

S V UNIVERSITY TIRUPATHI, ANDHRA PRADESH).

EMAIL ID: eganeshkumar1@gmail.com

***Abstract:***

Public Key Encryption with Equality Test (called PKE-ET) allows anyone to perform an equal test between two messages encrypted under separate public keys. During the comparison, information about Trapdoor as well as cipher features will not be exposed to this cloud server. Furthermore, according to the decisive billionaire Diffie-Hellman under, it has been proven to be safe against the selective plaintext attack in the standard model. Finally, theoretical performance analysis and experimental simulation indicate the feasibility and practicality of our proposed scheme.

***Keywords:*** *Cloud computing, flexible data search, privacy-preservation, predicate encryption with equality test, standard model..*

1. INTRODUCTION:

With the advent of the big data age, huge amounts of data are being collected and analyzed across a variety of application scenarios, including the Smart City Intelligent Transport System (ITS) and Smart Grid. To provide useful information to the individual and to society, storing and processing mass data has become an essential task. Fortunately, cloud computing is a novel computing example that enables ubiquitous access to infinite storage and computing resources at minimal operating cost. Considering the good potential of cloud computing, individuals and organizations have recently become increasingly inclined to remotely store and process their data with cloud computing support.

Despite the enormous advantages of cloud computing, it is prudent to rethink traditional methods for maintaining data privacy, integrity, and reliability, as the cloud server is usually provided by a trusted enterprise or corporation. Encryption — and then our outsourcing — is a common way to ensure the confidentiality of data stored on a cloud server. In particular, public-key encryption (PKE) has been widely used to ensure the confidentiality of outsourced data. To securely share sensitive data with specific users, the data holder can encrypt this data under the desired receiver's public key and deliver the corresponding cipher to the cloud server. In this way, only the designated receiver can access the data by decrypting it with his / her own private key. However, the data owner must perform the public-key encryption algorithm multiple times if the data needs to be shared with multiple users. To provide one-to-many encryption, the primitive of feature-based encryption (ABE) was proposed by Sahay and Waters as an extension of the common PKE. In the ABE mechanism, the user's secret key and cipher are labeled with detailed features and accessibility, respectively. The user can decrypt the cipher if the features associated with this user satisfy the cipher accessibility policy. With ABE's support, secure and flexible data sharing in cloud computing is easily achieved.

1. RELATIVE STUDY:
2. *UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges*

Without a reliable and efficient transport system, a smart city would not exist. This requirement makes ITS the key to any smart city concept. Legacy ITS technologies are deployed worldwide in smart cities, relying on the effective integration of next-generation ITS connected and autonomous vehicles, two of the most widely tested technologies in many cities around the world. While these two emerging technologies are crucial in launching fully automated transportation systems, there is still a need to automate other road and transportation components. To this end, UAVs are embedded in many ITS application domains because of their mobility, autonomous operation and communication/processing capabilities. This article describes the ITS applications that UAVs can use, and highlights the potential and challenges of UAV-enabled ITS for the next generation of smart cities.

1. *Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms*

Smart City is one of the most promising, popular and challenging Internet of Things (IoT) applications. In the last few years, the smart city concept has played an important role in the education and industry sectors, including the development and deployment of various middleware platforms and IoT-based infrastructure. However, this deployment follows different approaches, and therefore, in a fragmented scenario, different IoT ecosystems cannot communicate between them. To fill this gap, Smart City needs to revisit IoT Semantics and provide a global general approach. For this purpose, this paper browses the semantic annotation of sensors in the cloud and can implement and consider innovative services by bridging the Cloud of Things (CoT) and IoT. Things like semantic can be considered for integrating different sources by defining the CoT example. We survey the Smart City vision, provide information on core needs, and highlight the benefits of integrating various IoT ecosystems in the cloud with this new CoT vision. This paper also discusses related challenges in this area of ​​research.

1. *Multi-Modal Design of an Intelligent Transportation System*

This paper proposes a novel Intelligent Transport System (ITS) utilizing cell systems, GPS tests, and a restricted ITS foundation for edge-level speed estimation in a heterogeneous rush hour gridlock circumstance. Bogus vehicle area information taken from the cell system can be handled to ascertain edge-level vehicle stream, space inhabitance and clog with a normal blunder of under 10%. For edge-level speed estimation, two models of its framework extension are proposed: the blockage inclusion model (Kokomo) and the edge coverage model (Ekomo). Speed ​​data of GPS probes is used to extend the speed estimates from a single infrastructure edge to a non-infrastructure edge (s). Kokomo's infrastructure requirement is stable but depends on the variability in ECOMO's edge congestion profile. COCOMO and ECOMO allow edge-level velocity estimation with a 90% error of 10%–22% and 10%–13%, respectively. Communication and storage of the proposed ITS will be required and the benefit of the traffic information generated will be evaluated.

1. *A Survey of Large Scale Data Management Approaches in Cloud Environments*

Throughout the late decades, the relentless augmentation of computational power has made a colossal downpour of data. Furthermore, continuous advances in web development have made it less complex for any customer to give and eat up content in any structure. This requires an adjustment in viewpoint in enlisting structure and tremendous scale data getting ready systems. Appropriated processing is joined to another perspective for the enlisting system. This model moves the territory of this structure to the framework to decrease the costs related to supervising gear and programming resources. This paper shows a total survey of the various procedures and frameworks for executing data heightened applications in the cloud, which are grabbing vitality in research and industry. We evaluate each arrangement's diverse structure decisions and its sensibility to help certain classes of uses and end-customers. Discusses the flexibility, strength, and future challenges of some open-completed issues and enormous scale data in the cloud. We include the best contender class features of uses that can be passed on in the cloud.

1. *Data Security and Privacy Protection Issues in Cloud Computing*

Everyone knows that cloud computing has many potential benefits and many enterprise applications and data are migrating to the public or hybrid cloud. With respect to some business-critical applications, companies, especially large enterprises, still don't move them to the cloud. The size of the market where cloud computing is shared is still far behind. From a consumer perspective, cloud computing security issues, particularly information security and security assurance issues, are the essential obstruction to the reception of distributed computing administrations. This paper gives a brief however thorough investigation of information security and protection insurance issues related with distributed computing at all stages of the data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work on data security and privacy protection issues in the cloud.

1. PROPOSED SYSTEM

In the proposed scheme, it is the first such scheme which meanwhile deals with these issues on both privacy protection of user attributes and flexible data search. Additionally, the rigorous security proof clearly states to prove that our scheme is IND-CPA secure in the standard model under decisional bilinear Diffie-Hellman assumption. Finally, we present theoretical comparisons and experimental simulations of the existing ABE-ETs and our AH-PE-ET scheme to indicate the feasibility and practicability of our proposed scheme.

1. ALGORITHMS:

Our proposed AH-PE-ET scheme is comprised of six algorithms: Setup, KeyGen, Trapdoor, Encrypt, Decrypt and Test. These algorithms are defined as follows:

1. Setup(λ): Produce the master secret key MSK, the public parameter PP based on a security parameter λ.
2. KeyGen(PP, MSK,→x ): Create the decryption secret key DSK for users based on the public parameter PP, the master key MSK and a predicate vector→x .
3. Trapdoor(PP, DSK,→x ): Generate the trapdoor TD for users based on the public parameter PP, the decryption key DSK and an attribute vector→x .
4. Encrypt(PP, M,→y ): Produce the ciphertext CT based on the public parameter PP, a plaintext message M and the predefined attribute vector→y .
5. Decrypt(CT,DSK): Decipher the ciphertext CT using the decryption secret key DSK.
6. Test(CTA,TDA, CTB,TDB): Decide whether MA in CTA is the same with MB in CTB using the trapdoor TDA and the trapdoor TDB.

CONCLUSION

In this paper, a novel AH-PE-ET scheme named attribute hiding predicate encryption with an equality test is formulated to provide the privacy preservation of user attributes and flexible search capability on ciphertexts simultaneously. With our introduced scheme, the data user, who features with a set of attributes, can delegate the capability of equivalence test to the cloud server for determining whether two expected ciphertexts contain the same plaintext message without leaking any attribute privacy and trapdoor privacy. To the best of our knowledge, this proposed scheme is the first such scheme which meanwhile deals with these issues on both privacy protection of user attributes and flexible data search. Additionally, the rigorous security proof is clearly stated to prove that our scheme is IND-CPA secure in the standard model under decisional bilinear Diffie-Hellman assumption. Finally, we present theoretical comparisons and experimental simulations of the existing ABE-ETs and our AH-PE-ET scheme to indicate the feasibility and practicability of our proposed scheme. Future work contains building one novel scheme that achieves the IND-CCA2 security in the standard model based on our present scheme.

REFERENCES

1. Y. Zhang, D. Zheng, and R. Deng,“Security and privacy in smart health: efficient policy-hiding attribute-based access control,” IEEE Internet of Things Journal, 2018, doi:10.1109/JIOT.2018.2825289.
2. H. Menouar, I. Guvenc, K. Akkaya, et al, “UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges”, IEEE Communications Magazine, vol. 55, no. 3, pp. 22-28, 2017.
3. M. Chaturvedi, S. Srivastava, “Multi-modal design of an intelligent transportation system”, IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 8, 2017
4. R. Petrolo, V. Loscri, N. Mitton, “Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms”, IEEE Transactions on Emerging Telecommunications Technologies, vol. 28, no. 1, 2017.
5. H. Xiong, J. Sun,“Comments on “Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing””, IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 4, pp. 461-462, 2017.
6. M. Ma, D. He, N. Kumar, et al., “Certificateless searchable public key encryption scheme for industrial internet of things”, IEEE Transactions on Industrial Informatics, 2017
7. Q. Jiang, M. Khan, X. Lu, J. Ma, D. He, “A privacy preserving three-factor authentication protocol for e-Health clouds”, The Journal of Supercomputing, vol. 72, no. 10, pp. 3826-3849, 2016.
8. I. Kim, S. Hwang, J. Park et al,“An Efficient Predicate Encryption with Constant Pairing Computations and Minimum Costs”, IEEE Transactions on Computers (TOC), vol. 65, no. 10, pp. 2947-2958, 2016.
9. X. Wang, F. Xhafa, W. Cai, et al., “Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage”, Computers & Electrical Engineering, pp. 56, no. 871- 883, 2016
10. H. Lee, S. Ling, J. Seo, et al., “Semi-generic construction of public key encryption and identity-based encryption with equality test”, Information Sciences, vol. 373, pp. 419-440, 2016.
11. F. Guo, W. Susilo, Y. Mu, “Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption”, IEEE Transactions on Information Forensics and Security (TIFS), vol. 11, no. 2, pp. 247-257, 2016.
12. K. Liang, W. Susilo, “Searchable attribute-based mechanism with efficient data sharing for secure cloud storage”, IEEE Transactions on Information Forensics and Security (TIFS), vol. 10, no. 9, pp. 1981-1992, 2015.
13. N. Cao, C. Wang, M. Li, K. Ren, W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data”, IEEE Transaction Parallel Distribute System (TPDS), vol. 25, no. 1, pp. 222- 233, 2014.
14. Q. Zheng, S. Xu, G. Ateniese, “VABKS: Verifiable attribute-based keyword search over outsourced encrypted data”, 33rd Annual IEEE International Conference on Computer Communication (INFOCOM 2014), pp. 522-530, IEEE, 2014
15. K. Yang, X. Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing”, IEEE Transactions on parallel and distributed systems, vol. 24, no. 9, pp. 1717-1726, 2013
16. D. Chen, H. Zhao, “Data security and privacy protection issues in cloud computing”, IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1, pp. 647-651, 2012.
17. Q. Tang, “Towards public key encryption scheme supporting equality test with fine-grained authorization”, Australasian Conference on Information Security and Privacy (ACISP), Springer, LNCS 6812, pp. 389-406, 2011.
18. D. Chen, H. Zhao, “Data security and privacy protection issues in cloud computing”, IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1, pp. 647-651, 2012.
19. Q. Tang, “Towards public key encryption scheme supporting equality test with fine-grained authorization”, Australasian Conference on Information Security and Privacy (ACISP), Springer, LNCS 6812, pp. 389-406, 2011.
20. M. Abdalla, M. Bellare et al., “Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions”, Journal of Cryptology, vol. 21, no. 3, pp. 350-391, 2008.