ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

SECURED DATA SHARING SCHEME IN CLOUD-ASSISTED IOT

S.Sathya Vignesh Kumar, S.Sankar Guru, A.S.Vijayarengaalwar,Dr.J.B.Shajilin Loret
(Department of IT, UG Scholar, Francis Xavier Engineering College, Tirunelveli, India)
(Asso.Professor, Department of IT, Francis Xavier Engineering College, Tirunelveli, India)

Abstract: The Internet of Things (IoT) is becoming a more popular technological trend, as delegating large IoT data processing to the cloud will significantly improve the efficiency of IoT applications.We suggest a versatile privacy-preserving data sharing (FPDS) scheme for cloud-assisted IoT in this paper.An IoT consumer can encrypt data and send it to a recipient using the FPDS scheme, which uses identity-based encryption.More significantly, an IoT user may define a fine-grained access policy to create a delegation credential, which can then be sent to the cloud, which will transform all encrypted data meeting the access policy into new ciphertexts readable by a new recipient.IoT users can exchange data that has been outsourced to the cloud in a scalable and privacy-preserving manner in this way.The FPDS scheme is safe against semi-trusted cloud and malicious IoT users, according to a detailed security review. Thorough theoretical and experimental.

INTRODUCTION

We are facing a dangerous incensement of publicly funded knowledge from a vast number of customers, thanks to the rapid development of systems management and mobile phones.These publicly available data can be tallied over time and mined by machine learning innovations to uncover substantial data and improve our lives. In recent years, an ever-increasing number of organisations have been distributing the publicly supported information to people in general for information mining purposes. Be that as it may, the promising focal points of information distributing and mining are at the danger of uncovering delicate data to information mineworkers.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

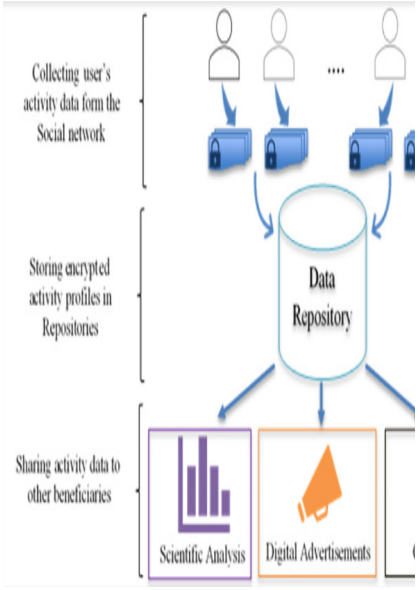
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

All these current frameworks center around utilizing cryptography or differential security to scramble or bother crude information on the information patron, which can ensure the genuine information independently, however isn't reasonable for the insurance of total measurements over publicly supported information, since the annoyance of crude information on every client would not influence the measurement estimation over publicly supported information. What's more, all current calculations under an untrusted server can't give solid assurance to constant information distributing. These issues rouse us to structure another differentially private system for continuous publicly supported measurable information distributing with the untrusted server.

To start with, how to total over publicly supported information without a focal confided in server? At the point when the server is known as untrusted, every client would not transfer the registration data to the server specifically any longer, which makes it hard to get the amassed insights for distribution. Second, how to guarantee the protection of every person? The main one that can be trusted by a client is itself. Despite the fact that a client must transfer its registration data to some place with the end goal of conglomeration, its character ought to be covered up so the transferred information would be not connected to the client. Finally, without a focal confided in server, the protection spending will most likely be allotted and utilized distributedly rather than a focal way. In this manner, it is trying to acknowledge w-occasion differential security for the constant discharged information without considering the server.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021



EXISTING SYSTEM

To ensure strong privacy, existing systems typically use a trusted server to aggregate spatiotemporal crowd-sourced data, then use a differential privacy mechanism to perturb the aggregate statistics before publishing.

Disadvantages:

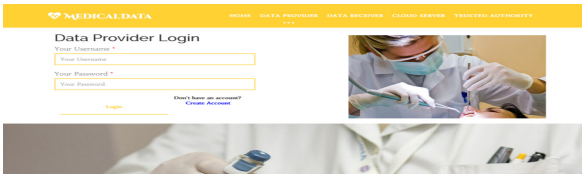
- High cost
- Data Overloading
- Data leakage

PROPOSED SYSTEM

In this project, we propose a flexible privacy-preserving data sharing (FPDS) scheme in cloud-assisted IoT. With the FPDS scheme, an IoT user can encrypt data to a recipient by using identity-based encryption.More significantly, the IoT user can define a fine-grained access policy to create a delegation credential, which can then be sent to the cloud to convert all encrypted data fulfilling the requirements.the access policy into new ciphertexts that square measure decipherable to a replacement recipient. during this method, IoT users will share the info outsourced to the cloud during a versatile and privacy-preserving manner.

INPUT IMAGE

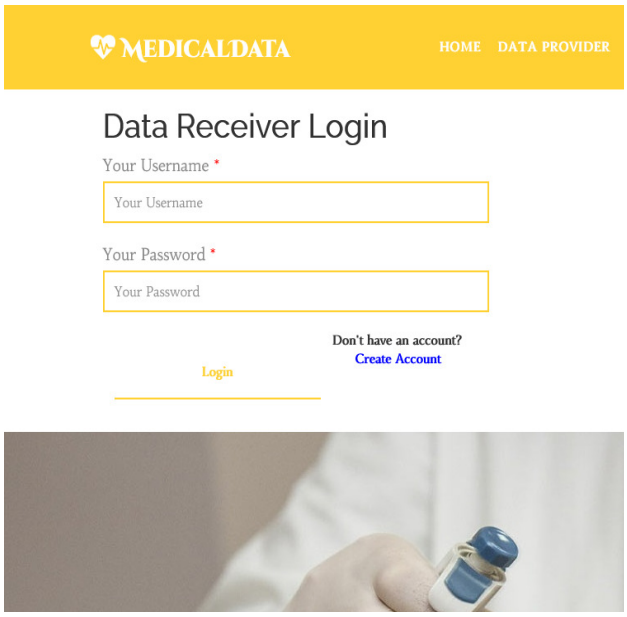
Step 1:



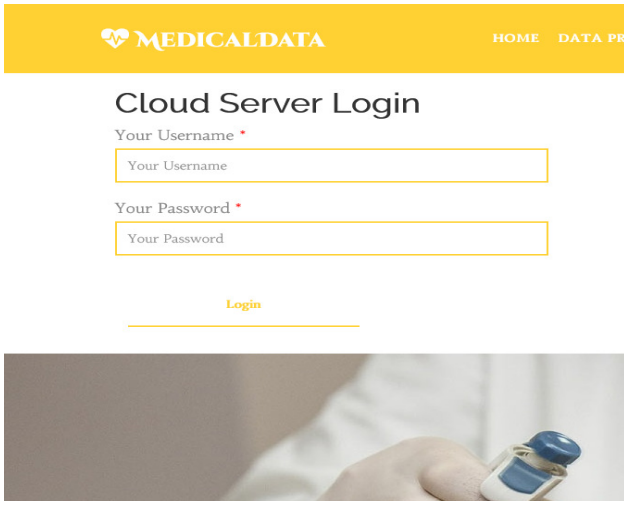
Step 2:

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

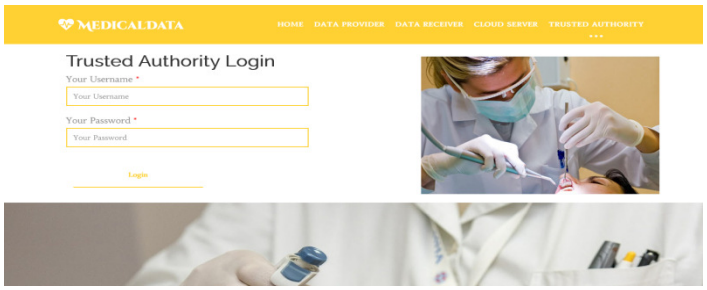
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021



Step 3:



Step 4:



Conclusion:

This paper proposed a flexible privacy-preserving data sharing (FPDS) scheme in cloud-assisted IoT. The FPDS scheme is characterized by employing identity-based encryption and linear secret sharing scheme to not only preserve the privacy of data outsourced to the cloud but also achieve flexible sharing of encrypted data. Detailed security analysis shows that the FPDS scheme is secure against semi-trusted cloud and malicious users. Thorough performance evaluation indicates the high efficiency of the scheme. The FPDS scheme allows to encrypt data with any recognizable identity and thus avoids complicated public-key certificates in usual secure storage systems. Similarly to the identity-based encryption, however, the FPDS scheme only allows to share data to one recipient, which makes it difficult to share data with a group of users. In our future work, we will explore more general solutions on basis of broadcast/attribute-based encryption, to support privacy-preserving data sharing for

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

multiple recipients in cloud-assisted IoT scenarios.

References:

[1] Foursquare, https://foursquare.com/.

[2] Waze, https://www.waze.com/zh/.

[3] P. Vo¨ lgyesi, A. Na´das, X. Koutsoukos, and A´ . Le´deczi, "Air quality monitoring with sensormap," in Proc. of IPSN'08. IEEE, 2008, pp. 529–530.

[4] W. Willett, P. Aoki, N. Kumar, S. Subramanian, and A. Woodruff, "Common sense community: scaffolding mobile sensing and analysis for novice users," Pervasive Computing, pp. 301–318, 2010.

[5] M.-H. Park, J.-H. Hong, and S.-B. Cho, "Location-based recommendation system using bayesian users preference model in mobile devices," in Proc. of IEEE UIC. Springer, 2007, pp. 1130–1139.

[6] K. Boriboonsomsin, M. J. Barth, W. Zhu, and A. Vu, "Eco-routing navigation system based on multisource historical and real-time traffic information," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 4, pp. 1694–1704, 2012.

[7] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," Scientific reports, vol. 3, 2013.

[8] C. Dwork, "Differential privacy," in Proc. of ICALP, 2006, pp. 1–12.

[9] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in Theory of cryptography, 2006, pp. 265–284.

[10] X. Xiao, G. Bender, M. Hay, and J. Gehrke, "ireduct: Differential privacy with reduced relative errors," in Proc. of ACM SIGMOD, 2011, pp. 229–240.

[11] J. Xu, Z. Zhang, X. Xiao, Y. Yang, G. Yu, and M. Winslett, "Differentially private histogram publication," The VLDB Journal, vol. 22, no. 6, pp. 797–822, 2013.

[12] M. Hay, V. Rastogi, G. Miklau, and D. Suciu, "Boosting the accuracy of differentially private histograms through consistency," Proc. of VLDB Endowment, vol. 3, no. 1-2, pp. 1021–1032, 2010.

[13] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias, "Differentially private event sequences over infinite streams," Proc. of VLDB Endowment, vol. 7, no. 12, pp. 1155–1166, 2014.

[14] Q.Wang, Y. Zhang, X. Lu, Z.Wang, Z. Qin, and K. Ren, "Rescuedp: Real-time spatio-temporal crowd-sourced data publishing with differential privacy," in Proc. of IEEE INFOCOM, 2016, pp. 1–9.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

[15] F. Armknecht and T. Strufe, "An efficient distributed privacypreserving recommendation system," in Proc. of IEEE Med-Hoc- Net, 2011, pp. 65–70.