International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

AN IDENTITY MANAGEMENT AND AUTHENTICATION SCHEME USING PRIVACY-AWARE PERSONAL DATA STORAGE (P-PDS) PROTECT USER PRIVACY FROM EXTERNAL APPLICATIONS

CHEREDDY DURGA BHAVANI [1], V.PRSANTHI [2]

[1] PG SCHOLAR, DEPT OF CSE,, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

[2]ASST. PROFESSOR [M.TECH] , DEPARTMENT OF CSE , ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

ABSTRACT: Recently, Personal Data Storage (PDS) has inaugurated a substantial change to the way people can store and control their personal data, by moving from a service-centric to a user-centric model. PDS offers individuals the capability to keep their data in a unique logical repository, that can be connected and exploited by proper analytical tools, or shared with third parties under the control of end users. Up to now, most of the research on PDS has focused on how to enforce user privacy preferences and how to secure data when stored into the PDS. In contrast, in this paper we aim at designing a Privacy-aware Personal Data Storage (P-PDS), that is, a PDS able to automatically take privacy-aware decisions on third parties access requests in accordance with user preferences. The proposed P-PDS is based on preliminary results presented in [1], where it has been demonstrated that semi-supervised learning can be successfully exploited to make a PDS able to automatically decide whether an access request has to be authorized or not. In this paper, we have deeply revised the learning process so as to have a more usable P PDS, in terms of reduced effort for the training phase, as well as a more conservative approach w.r.t. users privacy, when handling conflicting access requests. We run several experiments on a realistic dataset exploiting a group of 360 evaluators. The obtained results show the effectiveness of the proposed approach.

1.INTRODUCTION

Nowadays personal data we are digitally producing are scattered in different online systems managed by different providers (e.g., online social media, hospitals, banks, airlines, etc). In this way, on the one hand users are losing control on their data, whose protection is under the responsibility of the data provider, and, on the other, they cannot fully exploit their data, since each provider keeps a separate view of them. To overcome this scenario, Personal Data Storage (PDS) [2]–[4] has inaugurated a substantial change to the way people can store and control their personal data, by moving from a service-centric to a user-centric model. PDSs enable individuals to collect into a single logical vault personal information they are producing. Such data can then be connected and exploited by proper analytical tools, as well as shared with third parties under the control of end users. This view is also enabled by recent developments in privacy legislation and, in particular, by the new EU General Data Protection Regulation (GDPR), whose art. 20 states the right to data portability, according to which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, thus making possible data collection into a PDS.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Up to now, most of the research on PDS has focused on how to enforce user privacy preferences and how to secure data when stored into the PDS. In contrast, the key issue of helping users to specify their privacy preferences on PDS data has not been so far deeply investigated. This is a fundamental issue since average PDS users are not skilled enough to understand how to translate their privacy requirements into a set of privacy preferences. As several studies have shown, average users might have difficulties in properly setting potentially complex privacy preferences [5]–[7]. For example, let us consider Facebooks privacy setting, where users need to configure the options manually according to their desire. In [8], [9], authors survey users awareness, attitudes and privacy concerns on profile information and find that only a small number of users change the default privacy preferences on Facebook. Interestingly, in [10], authors find that even when users have changed their default privacy settings, the modified settings do not match the expectations (these are reached only for 39% of users). Moreover, another survey in [11] has shown that Facebook users are not aware enough on protection tools that designed to protect their personal data. According to their study the majority (about 88%) of users had never read the Facebook privacy policy.

2.LITERATUREREVIEW

Learning privacy habits of pds owners, by B. C. Singh, B. Carminati, and E. Ferrari
The concept of Personal Data Storage (PDS) has recently emerged as an alternative and innovative way of managing personal data w.r.t. the service-centric one commonly used today. The PDS offers a unique logical repository, allowing individuals to collect, store, and give access to their data to third parties. The research on PDS has so far mainly focused on the enforcement mechanisms, that is, on how user privacy preferences can be enforced. In contrast, the fundamental issue of preference specification has been so far not deeply investigated. In this paper, we do a step in this direction by proposing different learning algorithms that allow a fine-grained learning of the privacy aptitudes of PDS owners. The learned models are then used to answer third party access requests. The extensive experiments we have performed show the effectiveness of the proposed approach.
openpds: Protecting the privacy of metadata through safeanswers by Y.-A. de Montjoye, E. Shmueli, S. S. Wang, and A. S. Pentland
The rise of smartphones and web services made possible the large-scale collection of personal metadata. Information about individuals' location, phone call logs, or web-searches, is collected and used intensively by organizations and big data researchers. Metadata has however yet to realize its full potential. Privacy and legal concerns, as well as the lack of technical solutions for personal metadata management is preventing metadata from being shared and reconciled under the control of the individual. This lack of access and control is furthermore fueling growing concerns, as it prevents individuals from understanding and managing the risks associated with the collection and use of their data. Our contribution is two-fold: (1) we describe openPDS, a personal metadata management framework that allows individuals to collect, store, and give fine-grained access to their metadata to third parties. It has been implemented in two field studies; (2) we introduce and analyze SafeAnswers, a new and practical way of protecting the privacy

of metadata at an individual level. SafeAnswers turns a hard anonymization problem into a more tractable security one. It allows services to ask questions whose answers are calculated against the metadata instead of trying to anonymize individuals' metadata. The dimensionality of the data shared with the services is reduced from high-dimensional metadata to low-dimensional answers that are less likely to be re-identifiable and to contain sensitive information. These answers can then be directly shared individually or in aggregate. openPDS and SafeAnswers provide a new way of dynamically protecting personal metadata, thereby supporting the creation of smart data-driven services and data science research.

3.EXISTING SYSTEM

Oort [27] is a user-centric cloud storage system that organizes data by users rather than applications, considering global queries which find and combine relevant data fields from relevant users. Moreover, it allows users to choose which applications can access their own data, and which types of data to be shared with which users. Sieve [28] allows user to upload encrypted data to a single cloud storage. It utilizes key-homomorphic scheme to provide cryptographically enforced access control.

Amber [29] has proposed an architecture where users can choose applications to manipulate their data but it does not mention either how the global queries work or how the application providers interact with. In [2], authors developed a user-centric framework that share with third parity only the answers to a query instead of the raw data. Mortier et al. [30] have proposed a trusted platform called Databox, which can manage personal data by a fine grained access control mechanism but do not focus on policy learning. Recently, [31] proposed a Block chain-based Personal Data Store (BC-PDS) framework, which leverages on BlockChain to secure the storage of personal data. However, all the above proposals focus on access control enforcement, whereas they do not consider user preference or policy learning.

Privacy preference enforcement have been also investigated in different domains, such as for instance social networks where most of the platforms offer users a privacy setting page to manually set their privacy preferences. Research works have tried to alleviate the burden of this setting, by exploiting machine learning tools. For instance, [32], [33] have investigated the use of semi-supervised and unsupervised approaches to automatically extract privacy settings in social media. In [34], authors have considered location based data. They have compared the accuracy of manually set privacy preferences with the one of an automated mechanism based on machine learning. The results show that machine learning approaches provide better result than user-defined policies. Bilogrevic et al. [35] also present a privacy preference framework that (semi)automatically predicts sharing decision, based on personal and contextual features. The authors focus only on g location information.

In the existing work, the system doesn't have strong techniques to implement Privacy-aware Personal Data Storage (P-PDS).

The system doesn't have active learning which is to select from the training dataset the most representative instances to be labeled by users.

4.PROPOSED SYSTEM

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

The system proposes a revised version of the ensemble learning algorithm proposed in [1], to enforce a more conservative approach w.r.t. users privacy. In particular, we reconsider how ensemble learning handles decisions for access requests for which classifiers return conflicting classes. In general, the final decision is taken selecting the class with the highest aggregated probabilities. However, this presents the limit of not considering user perspective, in that, it does not take into account which classifier is more relevant for the considered user.

To cope with this issue, we propose an alternative strategy for aggregating the class labels returned by the classifiers. According to this approach, we assign a personalized weight to each single classifier used in ensemble learning. We also show how it is possible to learn these weights from the training dataset, thus without the need of further input from the P-PDS owner. Experiments show that this approach increases users satisfaction as well as the learning effectiveness.

PDS able to automatically take privacy-aware decisions on third parties access requests requires further investigation.

The system proposes a revised version of the ensemble learning algorithm proposed in this system, to enforce a more conservative approach w.r.t. users privacy.

5. SYSTEM ARCHITECTURE:

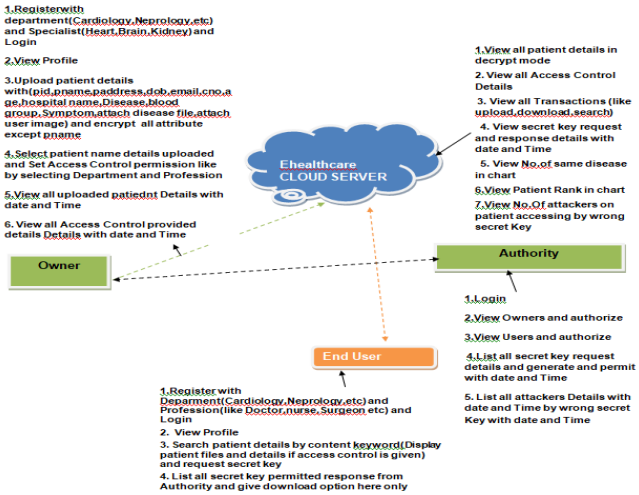


Fig 4.1 architecture Diagram

6.IMPLEMENTATION

DATA OWNER

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Register with department(Cardiology,Neprology,etc) and Specialist(Heart,Brain,Kidney) and Login and View Profile ,Upload patient details with(pid,pname,paddress,dob,email,cno,age, hospital name,Disease,blood group,Symptom,attach disease file, attach user image) and encrypt all attribute except pname ,Select patient name details uploaded and Set Access Control permission like by selecting Department and Profession and View all uploaded patient Details with date and Time ,View all Access Control provided details with date and Time.

EHEALTHCARE CLOUD SERVER

In this module the cloud will authorize both the owner and the user and also performs the following operations such as View all patient details in decrypt mode and View all Access Control Details, View all Transactions (like upload, download, search) and View secret key request and response details with date and Time View No.of same

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

disease in chart, View Patient Rank in chart and View No.Of attackers on patient accessing by wrong secret Key

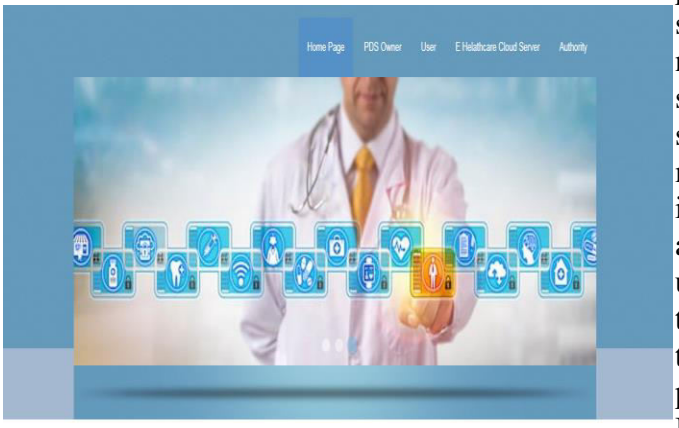
AUTHORITY

In this module, the Authority performs the following operations such as Login ,view Owners and authorize and View Users and authorize,List all secret key request details and generate and permit with date and Time and List all attackers Details with date and Time by wrong secret Key with date and Time.

END USER

In this module, the user has to register to cloud and log in and performs the following operations such as Register with Deparment(Cardiology,Neprology,etc) and Profession(like Doctor,nurse,Surgeon etc) and Login ,View Profile and Search patient details by content keyword(Display patient files and details if access control is given) and request secret key and List all secret key permitted response from Authority and give download option here only.

7. SCREEN SHOTS



8.CONCLUSION

Sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. The photo that a user wants to share is temporarily holden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserving and information sharing, we propose a service provider-assisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuning method. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user's privacy loss, and adaptively setting the threshold is necessary for the publisher to balance between privacy preserving and photo sharing.

In current study, we mainly focus on the sharing between one publisher and one

receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we'd like to investigate such a one-to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

BIBILOGRAPHY

[1] W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," Bus. Horiz., vol. 52, no. 4, pp. 357–365, 2009.

[2] A.M. Kaplan andM. Haenlein, "Users of the world, unite! The challenges and opportunities of social media," Bus. Horiz., vol. 53, no. 1, pp. 59–68, 2010.

[3] J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue," Telecommun. Policy, vol. 39, pp. 745–750, 2015.

[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.

[5] N. Senthil Kumar, K. Saravanakumar, and K. Deepa, "On privacy and security in social media a comprehensive study," Procedia Comput. Sci., vol. 78, pp. 114–119, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211

[6] C. Fiesler et al., "What (or who) is public?: Privacy settings and social media content sharing," in Proc. ACM Conf. Comput. Supported Cooperative Work Social Comput., Mar. 2017, pp. 567–580.

[7] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proc. 18th ACM Int. Conf. World Wide Web, Apr. 2009, pp. 521–530.

[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proc. 27th ACM Annu. Comput. Secur. Appl. Conf., Dec. 2011, pp. 103–112.

[9] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Trans. Knowl. Data Eng., vol. 28, no. 7, pp. 1851–1863, Jul. 2016.

[10] L. Xu et al., "Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards," IEEE Trans. Inf. Forensics Security, vol. 12, no. 2, pp. 271–285, Feb. 2017.

[11] M. Duggan and J. Brenner, "The demographics of social media users, 2012," vol. 14, Pew Research Center's Internet & American Life Project, 2013.

[12] L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure JPEG," in Proc. Comput. Commun. Workshops, 2015, pp. 185–190.

[13] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Trans. Dependable Secure Comput., vol. 14, no. 2, pp. 199–210, Mar. 2017.

[14] J. Bethencourt, A. Sahai, andB.Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[15] C. Ma, Z. Yan, and C.W. Chen, "Scalable access control for privacy-aware media sharing," in IEEE Trans. Multimedia, vol. 21, no. 1, pp. 173–183, Jan. 2019.

[16] P. Ilia, I. Polakis, E.Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," in Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur., 2015, pp. 781–792.
[17] L. Chao,W.Wang, and Y. Guo, "A fine-grained multiparty access control model for photo sharing in OSNS," in Proc. IEEE 1st Int. Conf. Data Sci. Cybersp., 2016, pp. 440–445.
[18] N. Vishwamitra et al., "Towards PII-based multiparty access control for photo sharing in online social networks," in Proc. 22nd ACMSymp. Access Control Models Technol., Jun. 2017, pp. 155–166.
[19] W. Sherchan, S.Nepal, and C. Paris, "Asurvey of trust in social networks," ACM Comput. Surv., vol. 45, no. 4, pp. 47:1–47:33, Aug. 2013.
[20] A. Datta, S. Buchegger, L. H. Vu, T. Strufe, and K. Rzadca, Decentralized Online Social Networks, New York, NY, USA: Springer, 2010.
[21] N. C. Rathore and S. Tripathy, "A trust-based collaborative access control model with policy aggregation for online social networks," Social Netw. Anal. Mining, vol. 7, no. 1, pp. 1–7, 2017.
[22] R. Gay, J. Hu, H. Mantel, and S. Mazaheri, "Relationship-based access control for resharing in decentralized online social networks," in Proc. Int. Symp. Found. Pract. Secur., 2017, pp. 18–34