Unspecified verification in health System using Time Constrained Access

[1] Puja Tiwari, [2,] Puja Patil [3] Harsha Ghadgee , [4] Prof Trupti Dange

Abstract:

Now a days there is a large amount of data generation and we have to store data securely. So here we are developing a healthcare application where we are providing a cloud for storage and provides services to patients. The sensitive data should be saved with the proper authentication. So security and privacy are the main issues while running the cloud applications. So here patients data can be handled without leaking their data. Here we are considering doctor, patient and admin. Here we are hiding the authentication to cloud server. The authentication server normally involves disclosing of the security like password and username. One easy way to protect their identities from server on cloud is anonymous authentication. The patients information can be tracked by the authentications server and by malicious attack the privacy can be breached. Some traditional approaches fail in the encryption and decryption process In this paper, we have proposed a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. In our proposed authentication scheme, we have utilized rotating group signature scheme based on Elliptic curve cryptography (ECC) to provide anonymity to the patients. To add an extra layer of protection, we have used The Onion Router (TOR) to provide privacy at the network layer. The performance of our scheme is evaluated by theoretical analysis which demonstrates that it resists various attacks and provides several attractive security features.

IndexTerms - Component,formatting,style,styling,insert.

I. INTRODUCTION

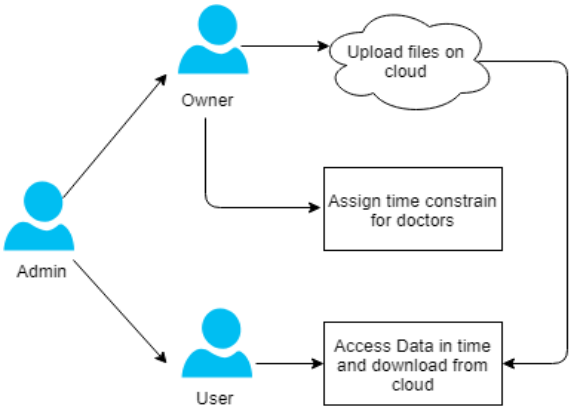
There is large amount of data generation. So we have to manage this data and cloud is used to outsource our data on cloud. To do this we are going to use Amazon s3 to access the data. Cloud is useful in different sectors like insurance, healthcare, and banking. It is useful because there is sensitive data on their server and we have to manage that data. So there is a need to secure this data. Sometimes patients don't want to disclose their data also they don't want to disclose their identities. The authentication process normally involves disclosing users' private information such as username and password to the authentication server. If the patient can be linked or tracked by the authentication server or malicious adversaries by their requests, their privacy can be breached. Most of the existing privacy preserving health care applications provide anonymity from the adversaries. However, very few of them provide anonymity from the authentication server. In this paper, we have proposed a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. In our proposed authentication scheme, we have utilized rotating group signature scheme based on

Elliptic curve cryptography (ECC) to provide anonymity to the patients. To add an extra layer of protection, we have used The Onion Router (TOR) to provide privacy at the network layer. The performance of our scheme is evaluated by theoretical analysis which demonstrates that it resists various attacks and provides several attractive security features. Recent advances in biosensors, wireless network and embedded systems have assisted the rapid development of a wide range of wearable and implantable sensors in the human body. To collect crucial health data such as blood pressure level, and heart rate, many smart phone based health applications have been developed in the recent past [1], [2]. The data from the sensors is sent to the cloud server, where hospitals have hosted their services for data processing. The data is analyzed to improve the level of healthcare given to the patients. An example of smart cloud based health applications is shown in Fig.1. Ideally, patients want hospitals to assist them with high efficiency without revealing patients' identities. The increasing necessity for massive computation and excessive amounts of storage, is driving the healthcare industry to use cloud based servers, because of many advantages they are offering, such as cost saving and scalability. However,

Keyword:
Anonymous authentication, rotating group signature, elliptic curve cryptography, smart health applications

Related Work:

The related work on anonymous authentication schemes can be broadly classified into public key cryptosystems (PKC) based schemes [13]–[19], identity based cryptosystems study of STASIS and LSA. These measures of semantic similarity can be applied to short texts for use in Conversational Agents (CAs). CAs are computer programs that interact with humans through natural language dialogue [7]. Tares Finlike proposed a system in which influence of transformation processes in higher education to lower academic standards, changes and deformation in ethical field of global and national higher education. We considered the genesis and modern standards of academic integrity [8]. schemes [4]–[5], pseudonyms based schemes [7], [11], combined scheme [12] using both identity based encryption and pseudonyms, and application oriented schemes [14]–[17]. Anonymous authentication schemes based on PKC in [13], [14] were infeasible for mobile networks because of the computational resources required by PKC modular exponentiation, which consume more resources than what a mobile device can offer. To minimize the computational requirements, various anonymous authentication schemes based on elliptic curve cryptosystem (ECC) have been proposed [15]–[20], which have better performance because of the smaller key size used in ECC. The performance of ECC based schemes are enhanced by identity based cryptosystems [17]–[20] over ECC. Unlike the traditional PKC, the identity based cryptosystems exploit public identity such as ID or email address as the user's public key to eliminate the cost related to the management of public key certificates, which is often desirable in mobile environments.



Motivation:

To secure data. And add privacy to data authentication. To minimize paper work. To prevent data from unauthorized access.

Mathematical Model

Let, S be the System Such that,
A= {I, O, F, success, failure}
Where,
I= Set of Input
O=Set of Output

F =Set of Function
Input: I=. Set of input i.e., text files
Function:

F1=Encryption Function (This function is used for files)

F2=Conjunctive Keyword Search Function(This function is used for searching)

F3=Time Enabled Proxy-Re-Encryption Function

F4= Decryption Function (This function is used for Decrypting files)

Output: O1=Success Case (It is the case when all the inputs are given by system are entered correctly)

O2=Failure Case (It is the case when the input does not match the validation Criteria)

Conclusion:

In this paper we are protecting the privacy of patients. And there is a minimization in the documents. And there is a overhead in key. The proposed scheme preserves the privacy of patients when they access the services hosted on the cloud.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on '**unspecified verification in health System using Time Constrained Access**

I would like to take this opportunity to thank my internal guide Prof Trupti Dange for giving me all the help and guidance I needed I am really grateful to them for their kind support. Their valuable suggestions were very helpful.
I am also grateful to HOD for her in dispensable support and suggestions.

Name of Students

[1] Puja Tiwari, [2,] Puja Patil [3] Harsha Ghadgee ,

REFERENCES:

[1] A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, "The pursuit of citizens' privacy: a privacy aware smart city is possible," IEEE Commun. Magazine, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[2] D. Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy, "Realtime tele-monitoring of patients with chronic heart-failure using a smartphone: lessons learned," IEEE Trans. on Affective Computing, vol. 7, no. 3, pp. 206–219, Apr. 2016.

[3] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Commun. Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, May 2013.

[4] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in Proc. Smart City Security and Privacy Workshop (SCSP-W), Apr. 2016, pp. 1–5.

[5] P. Gope and T. Hwang, "Untraceable sensor movement in distributediot infrastructure," IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Jun.2015.
[6] X. Su, J. Hyysalo, M. Rautiainen, J. Riekki, J. Sauvola, A. I. Maarala, H. Hirvonsalo, P. Li, and H. Honko, "Privacy as a service: Protecting the individual in healthcare data processing," Comput., vol. 49, no. 11, pp. 49–59, Nov. 2016.

[7] W. Lei, Y. Li, Y. Sang, and H. Shen, "A secure anonymous authentication scheme for electronic medical records system," in Proc. 13th Int. Conf. on e-Business Engineering, Nov. 2016, pp. 48–55.

[8] V. Sucasas, G. Mantas, A. Radwan, and J. Rodriguez, "An oauth2-based protocol with strong user privacy preservation for smart city mobile ehealth apps," in Proc. IEEE Int. Conf. on Commun., May 2016, pp. 1–6.

[9] R. Fernando, R. Ranchal, B. An, L. B. Othman, and B. Bhargava, "Consumer oriented privacy preserving access control for electronic health records in the cloud," in Proc. IEEE 9th Int. Conf. on Cloud Computing, Jun. 2016, pp. 608–615.

[10] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," IEEE Access, vol. 4, pp. 1821–1834, Apr. 2016.

[11] H. Xiong, J. Tao, and C. Yuan, "Enabling telecare medical information systems with strong authentication and anonymity," IEEE Access, vol. 5, pp. 5648–5661, 2017.

[12] X. Li, S. Tang, L. Xu, H. Wang, and J. Chen, "Two-factor data access control with efficient revocation for multi-authority cloud storage system," IEEE Access, vol. 5, pp. 393–405, 2017.

[13] J. Zhu and J. Ma, "A new authentication scheme with anonymity for
wireless environments," IEEE Trans. on Consumer Electron., vol. 50, no. 1, pp. 231–235, Feb. 2004.

[14] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," Comput. Security – ESORICS 98, pp. 277–293, 1998.

[15] C. Yang, W. Ma, and X. Wang, "Novel remote user authentication scheme using bilinear pairings," Lecture Notes in Comput. Science, vol. 4610, p. 306, 2007.

[16] P. E. Abi-Char, A. Mhamed, and E.-H. Bachar, "A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications," in Proc. Int. Conf. on Next Generation Mobile
Applications, Services and Technologies, 2007, pp. 235–240.

[17] L. Zhang, S. Tang, and H. Luo, "Elliptic curve cryptography-based authentication with identity protection for smart grids," PloS one, vol. 11,no. 3, pp. 1–15, 2016.

[18] Y.-M. Tseng, T.-Y. Wu, and J.-D. Wu, "A mutual authentication and key exchange scheme from bilinear pairings for low power computing devices," in Proc. 31st Annu. Int. Conf. on Comput. Software and Applications, vol. 2, Jul. 2007, pp. 700–710.

[19] J.-H. Yang and C.-C. Chang, "An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Comput. and Security, vol. 28, no. 3, pp. 138–143, Jun. 2009.

[20] X. Cao, X. Zeng, W. Kou, and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," IEEE Trans. on Vehicular Technology, vol. 58, no. 7, pp. 3508–3517, Sep. 2009.