Smart Anonymous Authentication Protocol for E-Governance

Akash Shirsath
Student of BE Computer
Engineering, BVCOE & RI
Nashik, India, University of Pune

Bhagyashree Bhujang
Student of BE Computer
Engineering, BVCOE & RI
Nashik, India, University of Pune

Karishma Sanap
Student of BE Computer
Engineering, BVCOE & RI
Nashik, India, University of Pune

Hemant D. Sonawavne
Head of Computer Engineering
BVCOE & RI, Nashik
India, University of Pune

ABSTRACT

Authentication services used many times a day. If there is no user authentication, then it would be impossible to use email accounts, discussion boards, e-banking or even electronic communication. On the other hand, It releases a lot of personal information during every authentication process. User login can be linked to used services and assets by service providers. The frequency of usage and therefore the map of our behavior on the Internet can be created to make more focused advertisement, to track us or even to steal our electronic identity. The purpose of this paper is to state the requirements and provide the initial design for an anonymous authentication scheme which prevents the leakage of private information. The new scheme, to be widely acceptable, must be beneficial for both users and service providers, who implement the authentication systems. Therefore the new authentication system must provide a feature for revealing dishonest users. These users can be eventually deanonymized and charged for damages.This paper provides such a responsibility-protecting feature in this new scheme.

Keywords

Anonymity, Privacy, Authentication, Efficiency, Responsibility

1. INTRODUCTION

Authentication services used many times a day. Without authentication, it would be impossible to use email accounts, discussion boards, e-banking or even electronic communication. On the other hand, It releases a lot of personal information during every authentication process. User login can be linked to used services and assets by service providers. The frequency of usage and therefore the map of our behavior on the Internet can be created to make more focused advertisement, to track us or even to steal our electronic identity. The purpose of this paper is to state the requirements and provide the initial design for an anonymous authentication scheme which prevents the leakage of private information. The new scheme, to be widely acceptable, must be beneficial for both users and service providers, who implement the authentication systems. Therefore the new authentication system must provide a feature for revealing dishonest users. Admin can block misbehaving user, This paper provides such a responsibility-protecting feature in this scheme.

Part of e-government is the services it provides. It is the possibility of accessing information and services of the public administration, 24 hours a day, 365 days a year, when it is needed, that is a reality that becomes evident. Online procedures and services make life easier and more convenient by offering the following advantages: 1) Citizens should not move in person. 2) No closing time, no waiting. 3) The execution of procedures is independent of the place. The possibility of vulnerabilities within these services should be considered when handling relevant and important information for citizens. In the case of leakage and theft of information is particularly compromising, since all such data can be acquired, stored and used by third parties for unauthorized or illegal activities, such as sending unsolicited advertising or obtain confidential banking information through deception.

2. METHODOLOGY

Firstly user will register to web application

1. Admin will authenticate user
2. After registering, user's identity will be encrypted by using AES algorithm. The purpose of identity encryption is to avoid attacks on common people.
3. User can complaint to web application by uploading image, gif etc.
4. User's complaint will get solved by his respective department.
5. After solving complaint, it is closed by admin.

3. RELATED WORK

Find anonymous authentication systems, e.g., the Scheme by Schaffer and Schartner (Schafferand Schartner, 2006), to be the most related systems. These schemes allow anonymous authentication but often rely on trusted third parties. The mentioned scheme is based on a device which must be trusted not to reveal private information. The second common problem is repeated authentication. Using existing schemes, the user cannot be authenticated infinitely many times without re-initialization.

The credential systems, represented by (Lysyanskaya, 200 I; Camenisch and Lysyanskaya, 2003; Camenischand Van Herreweghen, 2002; Bichsel ET aI. 2009), are also usable for anonymous authentication. Although these systems can be used in many scenarios for privacy protection, only some of them provide real identity revelation of dishonest users. Such features provided in theory (Camenisch and Lysyanskaya, 2003) but the implementation would be very inefficient or even impossible on current smart-cards.

4. SYSTEM ARCHITECTURE

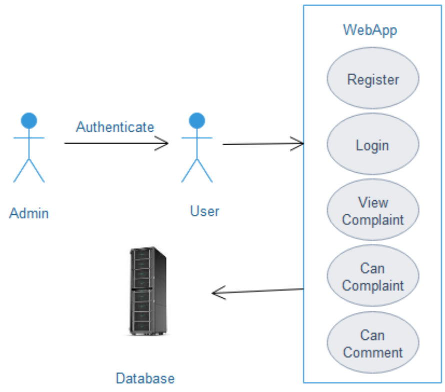


Fig 1: System Architecture

5. ALGORITHM

1. Advanced encryption standard:

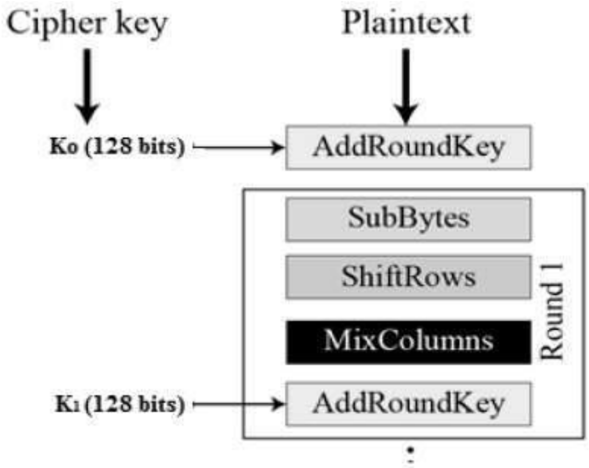
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

5.1 Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −



AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

6. CONCLUSION

The paper introduced a new scheme for anonymous

Authentication. Unlike related work, our scheme combines Features required by both users and service providers. Using our scheme, the user can be authenticated without real identity revelation and the service provider can be sure about the control over his assets. We provided the communication pattern of the scheme and identified cryptographic primitives used. The scheme is very efficient and implementable on weak devices like smart-cards. Nevertheless, the works are still in progress and we expect a significant performance improvement. Our goal is to reach 30 % performance advantage over related schemes, an increase which is achievable based on the theoretical construction of the scheme. Moreover, we are Working on the support of "attribute authentication", Where users can prove not only the group membership But any attribute ownership (e.g., driving license, age, Citizenship).

7. REFERENCES

[1] Bao, F. (2000). An efficient verifiable encryption schemefor encryption of discrete logarithms. In Schneier, B.and Quisquater, 1.-1., editors, Smart Card. Research and Applications, volume 1820 of Lecture Notes inComputer Science, pages 2 13-220. Springer.

[2] Bichsel, P., Camenisch, 1 GroB, T., and Shoup, V. (2009).Anonymous credentials on a standard java card. In Proceedings of the 16th ACM conference onCompute and communications security, CCS '09, pages 600--610, New York, NY, USA. ACM.

[3] Camenisch, 1. And Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In Proceedings of the3rd international conference on Security in communicationnetworks, SCN'02, pages 268-289,Berlin,

[4] Heidelberg. Springer-Verlag.Camenisch, 1. And Stadler,M. (1997). Proof systems forGeneral statements about discrete logarithms. Technicalreport.

[5] Camenisch, 1. And Van Herreweghen, E. (2002). Design and implementation of the idemix anonymous credential system. In Proceedings of the 9th ACM conferenceon Computer and communications security, CCS '02, pages 2 1-30, New York, NY, USA. ACM.

[6] Dingledine, R., Mathewson, N., and Syverson, P. (2004).Tor: The second-generation onion router. In Proceedings of the 13 th Usenix Security Symposium.

[7] Lysyanskaya, A. (200 I). An efficient system fornontransferable anonymous credentials with optionalAnonymity revocation. Pages 93- 1 18. Springer.

[8] Schaffer, M. and Schartner, P. (2006). Anonymous authenticationwith optional shared anonymity revocation andlinkability. In Smart Card Research and

AdvancedApplications, volume 3928 of Lecture Notes inComputerScience, pages 206-22 1. Springer Berlin / Heidelberg.

8. AUTHOR'S PROFILE

Akash Sirsath he is Engineering student of Computer Engineering at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest in the field of Innovation in Application

Bhagyashree Bhujang she is Engineering student of Computer Engineering at Brahma Valley College of Engineering and Research Institute, Nasik under University of Pune. Her interest in the field of Innovation in Application.

Karishma Sanap she is Engineering student of Computer Engineering at Brahma Valley College of Engineering and Research Institute, Nasik under University of Pune. Her interest in the field of Innovation in Application.

Hemant D.Sonawavne, ME, BE Computer Engg. Was educated in Pune University. Presently he is working as a Head of Computer Department of Brahma Valley College of Engineering and Research Institute, Nasik, Maharashtra, India. he has presented papers at National and International conferences and also published papers in National and International Journals on various aspects of Computer Engineering and Networks. His areas of interest include Computer.

[9] Schnorr, C. P. (1991). Efficient signature generation bysmart cards. Journal of Cryptology, 4: 16 1- 174