Research Paper

Volume : 4 | Issue : 3 | March 2015 • ISSN No 2277 - 8179

Secured Authentication for Aadhaar Card Through Sensory Information Using Mobile Phone

Engineering

KEYWORDS : Aadhaar card, Authentication, Message Authentication Code

U.Narmatha PG Scholar, S.A Engineering College, Chennai Department of computer Science and Engineering

Mr.S.Muthukumarasamy Assistant Professor, S.A Engineering College, Chennai Department of computer Science and Engineering

ABSTRACT

Government of India is issuingan AADHAAR card to every individual resident, which contains a 12 digit unique identification number. Aadhaar card is being issued by Unique Identification Authority of India as identity proof for availing all service of government and non-government. Aadhaar card is single all-purpose use card provided with highly secured authentication which requires each time to verify three to four attributes of the user. Currently, authentication is provided by combination of any of the following attributes -personal information, bio metric, demographic and One Time Password (OTP). The bio metric authentication is costly and cannot be shared with trusted persons in case of emergency requirements. The authentication through OTP is also unsecured,if mobile phone and aadhaar card is stolen. The combination of these authentications makes the user authentication process complex and time consuming. So here, a simple dynamic authentication is provided based on sensory information and implementing message Authentication code on generated OTP. This proposed system provides a highly secured and simple authentication for smartcard.

INTRODUCTION

Unique identification authority of India is issuing a 12 digit unique identification number on behave of government of India to every resident Indian including children and infant. This unique number will serve as identify proof and address proof anywhere inside the country of India. The 12 digit number will remain valid for life time and help providing access to service in government and non-government. It will be used by all identity based service like ration, passport, etc. It is a voluntary service that every individual can avail on basis of demographic and biometric information. The name Aadhaar depicts the fundamental role of UIDAI as a universal identity organization, a foundation over which public and private agencies can build services and applications that benefit people across India.

Aadhaar card usage is mainly for micropayments. To diminish the shortage of financial access in India, it has been focused on improving the financial services in innovative ways through without unnecessary extras accounts, the favorable of banking and ATM rules. Advanced technology like core banking, ATMs, and mobile connectivity have lager impact on banking. Mobile phones substantially increase financial services across India, with these technologies the need for banks has been reduced and banks are consequently providing services through internet and mobile banking. In addition to ATMs, these options have made banking affordable and accessible for many non-poor urban people across the country.Another limitation is the cost of providing banking services to the poor who manage in smaller amounts (micropayments). These payments are considered unattractive as transaction costs are too high to bear. The aadhaar card helps poor people establish their identity to banks and banks would be able to scale up their branch-less banking deployments to a wider population at lower cost. An efficient, cost effective payment solution is a terrible necessity for supporting financial addition. The Aadhaar card authentication mechanism provides the chosen micropayment solution which brings low-cost access to financial services to everyone at short distance from home.

EXISTING SYSTEM

Aadhaar authentication process involves in verifying the 12 digit unique Aadhaar number, and other attributes like demographic, biometrics and OTP. These verification attributes are recorded in Central Identities Data Repository (CIDR) of Unique Identification Authority of India (UIAI). When they submit these records for verification it would be verified against the stored record in database and if the records match then CIDR would send a responds "yes "otherwise "no". And the response would not return any personal identities. This authentication is to permit people to confirm their identity. Also helps service providers to confirm the residents to deliver services and offer access to benefits.

DRAWBACKS

When offering service the authentication is provided by five methods

- First method: Using aadhaar card number and demographic information.
- Second type is to sending one time password to the user personal mobile phone.
- Third type is to use one of the biometric modalities like finger printer or iris.
- Fourth type uses one time password as first factor and one of biometric authentication as second factor.
- Fifth using three attributes that is one time password, iris and finger prints for authenticating people.
- So this makes
- The above type will make the authentication process
- Lengthier and time consuming
- Complex
- OTP is unsecured if the unauthorized person owes the user mobile phone.
- Bio metric is costly and cannot be shared with trusted person in emergency
- These drawbacks will be address and solved in proposed system.

PROPOSED SYSTEM

The proposed system aims to provide simple highly secured authentication for aadhaar card by providing sensor based authentication and generating one time based authentication by implementing Message authentication code. By providing this sensor based authentication the process becomes simple and highly secured with less expensive.

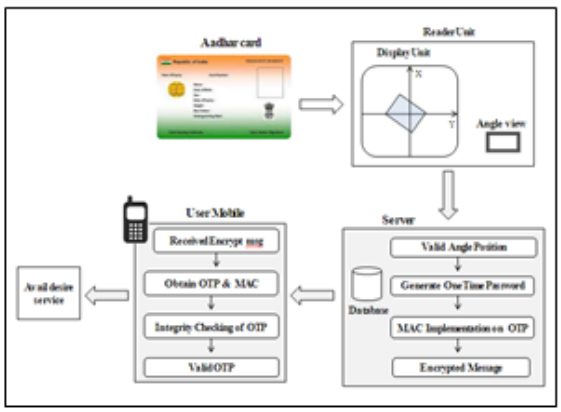

Fig1: Overall Architecture

Sensor Based Authentication

The sensor based authentication is provided by using accelerometer sensor. An accelerometer sensor will be placed inside the aadhaar card. It will authenticate the aadhaar card based on the position (axis) of the card placed. The sensor authentication is provided by setting up a fixed axis position for sensor inside that aadhaar card based on the angle of the card placed (within 360 degrees). The reader unit will read the angle of the aadhaar card when placed on the display unit. After reading the angle position of the aadhaar card, it will forward that information for server. If the server authenticates the position then the server will proceed to generate and One time password.

The 12-digit uniquenumber of aadhaar card and its corresponding angle i.e. the sensor's axis position is stored in its database. So the information forwarded by the reader unit to server will be verified with the server database. If the information matched any record in the database then the aadhaar card will be authenticated.

The advantage of the system is user themselves will setup angle position for the card. This is like setting up a password and personal identification number. The reader unit has a display unit where user can view the two dimensional (x, y) axes.When the user places the aadhaar card on that display unit it will give the angle position of the card. The angle will be displayed only to the user in small area which would be viewed only by the user which is protected from other peeping on it. So when user wants to fix position for their aadhaar card, they have place the aadhaar card on the display unit andchoose an angle of their choice and register it for their aadhaar card. This angle position will be recorded for the user along with the 12-digit unique identification number in the server database. When user want to avail a service the user has to place their aadhaar card in angle position they fixed for it, only then the card will be authenticated. This protects the unauthorized person using the card in case of availing financial service like banking etc.

MAC Implementation on generated OTP

Once the aadhaar card position is authenticated the server will generate a onetime password by implementing MAC. This will provide a high security to one time password which is generated by server and sent to user mobile phone.

Message authentication code is a mechanism or service used to provide integrity and authenticity assurance of a message. Message authentication code is an algorithm that requires using two common secret key between sender and receiver. A variable-length message and secret keys are taken as input to produce an authentication code to verify the integrity of the message. In proposed system, MAC is implemented on One Time Password (OTP). On validating the IMSI number of user mobile, server generates a one time password and sends it to user's mobile. With the help of this OTP only the user could avail the smart card service. By implementing MAC on OTP, the integrity and authentication is preserved. So, it confirms user that it is safe to use the OTP to avail the service, as it is secured from intentional or accidental changes.

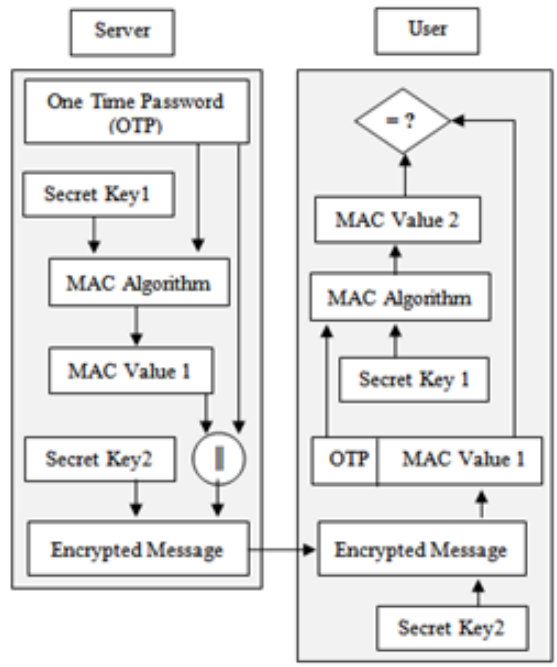

Fig 2. MAC implementation

The Figure2 illustrates the implementation of MAC on OTP. After generating OTP, server perform MAC algorithm with two secret keys which is known only to the sender and receiver. At the server end, the generated OTP is applied to MAC algorithm using secret key 1 to produce MAC value 1 then, this MAC value 1 is concatenated with the OTP to produce concatenated message. Now the secret key 2 is applied to concatenated message to produce encrypted message. At client end, user receives the encrypted message alone and they perform the reverse operation to obtain the OTP. Secret key 2 is applied to the received encrypted message to produce the OTP and MAC value 1. Then, user performs MAC algorithm by applying secret key 1 on OTP to produced MAC value 2 and it compares the received MAC value 1 with generated MAC value 2. So the user is able to check the integrity and authenticity of the OTP before using it to avail the service.

This MAC implementation, enormously enhance the security level of the OTP. if the unauthorized person succeeds in the sensor based authentication of aadhaar card, they required to complete the authentication by obtaining the OTP from the encrypted message to availing the service for which they required user's mobile. Even if they obtain the user mobile, they required to know the secret keys to obtain the OTP from received encrypted message in user's mobile.

CONCLUSIONS

The proposed work will provide a simple and highly secured authentication for aadhaar card.

This sensor based authentication requires less expense and it prevents the unauthorized authentication as the user has to

Volume : 4 | Issue : 3 | March 2015 • ISSN No 2277 - 8179

know the exact authenticating angle position of the aadhaar card. To thwart the success in sensor based authentication, an OTP is sent to the user mobile phone in a form of encrypted message. This challenges the unauthorized person, as they required knowing two secret to obtain the OTP from the received encrypted message. So this makes the authentication process very simple highly secured for user. Andavoid cost of bio metric authentication.

REFERENCE

[1] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," Proc. Fifth Int'l Conf. Pervasive Computing, pp. 144-161, 2007. | [2] J. Kong, H. Wang, and G. Zhang, "Gesture Recognition Model Based on 3D Accelerations," Proc. IEEE Fourth Int'l Conf. Computer Science & Education (ICCSE), 2009. | [3] S.Mitra and T.Acharya, "Gesture Recognition: A Survey," IEEE Trans. Systems, Man and Cybernetics, vol. 37, no. 3, pp. 311-324, May 2007. | [4] T. Helleseth and T. Johansson, "Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 31-44, 1996. | [5] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family," J. Math. Cryptology, vol. 4, no. 2, 2010. | [6] D. Ma and N. Saxena, "A Context-Aware Approach to Defend against Unauthorized Reading and Relay Attacks in RFID Systems," Security and Comm. Networks, doi: 10.1002/sec.404, | [7] V. Shoup, "On Fast and Provably Secure Message Authentication Based on Universal Hashing," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 313-328, 1996. | [8] T. Helleseth and T. Johansson, "Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 31-44, 1996.