ANONYMOUS DUAL-FACTOR AUTHENTICATION USING SMART CARD

Kambaduru sai Vikas kumar¹
U.G Student, Dept. Of CSE,
Sathyabama Institute of Science and Technology, Chennai, India
¹sai355205@gmail.com

Kotte Bhavani sai nikhil²
U.G Student, Dept. Of CSE,
Sathyabama Institute of Science and Technology, Chennai, India
²sainikhilkotte999@gmail.com,

Albert Mayan J³
Assistant Professor, Dept. Of CSE,
Sathyabama Institute of Science and Technology, Chennai, India
³albertmayan@gmail.com

Abstract—Nowadays, IT-enabled service gains more attention due to easy to access resources from a remote place. IT-enabled services extend their service to all kind of business and personal related applications like e-commerce, e-business, e-transactions, e-healthcare, etc.. Such development parallelly brings a need for security concern. The system as part proposes a technique to ensure access security. It uses a two-factor authentication scheme using Elliptic Curve Cryptography thereby providing a secured and multi-level authentication service. Authentication is based on two-factor authentication with smart card and binary code, which provides high security with minimum computational cost. The scheme generates a new session key for every new session with a fresh timestamp and nonce value.

Keyword----Radio Frequency Identification (RFID), smartcard, MYSQL database, Elliptic Curve Cryptography (ECC).

1. Introduction

Anonymous dual-factor authentication that uses passwords and smartcard could preserve user privacy and reduce the risk of using a single authentication factor. Compared to previous security processes this will be more secure because of using the binary code as encryption and decryption. The first password authentication scheme based on a smart card without a confidential verification table stored on the server, which is a key advantage of two-factor schemes compared to confidential password table for this last on the server. Mobile computing devices are of great
security concern not only because of the data stored on them, but also for that they may provide access to other services that store or display non-public data. For almost all these transactions, mutual authentication and user privacy are required in the key exchange before remote servers start providing services to users.

In particular, authentication and privacy play an important role in applications for industrial networks, wireless sensor networks, distributed networks, as well as RFID systems. Due to the advantages on portability and usability, most proposed authenticated key exchange (AKE) protocols support two factor authentication using passwords and smart cards. Binary code as a key makes authentication more secure. Tapping system will be easy for the user to use or access smart card. Secure level will be very high with the combination of smart card and binary code usage. Extending the security model of AKE to support user anonymity and resist lost-smart-card attack, and then propose a dynamic ID-based Anonymous Two-Factor protocol which satisfies all the following properties: (1) Security against various attacks including de-synchronization attack, lost-smart-card attack and offline dictionary attack; (2) User anonymity and un-traceability; (3) Perfect forward secrecy; (4) No long-term public key; (5) No centralized password storage, and support user password change and smart card revocation; (6) Provable security in extended security model. The rest of the paper is as follows: section II describes the Literature survey of previous papers, section III explains the proposed model for the paper and the dataset, it is processing, section IV describes the methodology used and the cryptography algorithm studied, section V presents the results and discussion, lastly section VI concludes the findings.

2. Literature Survey

An Effective 3-factor authentication for Secure Communication using Improved Smart Card Authentication was latently published in 2016. It provides Secure Communication from various attacks and low Communication and Computation cost.

Intercept Behaviour Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack was proposed in 2015. Asymptotic intercept probability analysis is performed to provide an imminent into the impact of the sensor scheduling on the wireless security.

Collaborative Localization and location verification in WSNs was proposed in 2015. It proposed the virtual force model to determine the location by incremental refinement.

Implementation of Single Sign-On Mechanism for Distributed computing was proposed in 2014. Implementation of Single Sign-On for distributed computing using user-id and password along with biometric verification.

Industrial Wireless Sensor Networks, Challenges, Design Principles, and Technical Approaches was proposed in 2014. Wired automation systems require expensive communication cables to be installed and regularity maintained and thus they are not widely implemented in industrial plants because of their high cost.
3. **PROPOSED MODEL**

Two-Factor Authentication Scheme is combined with smart card and binary code. Elliptic Curve Cryptography is used for encrypting binary code. This algorithm is proposed so that encryption will be more secured. This scheme is verified with Random Oracle Model for real-time security proof. This requires a nominal amount of computational cost and communication cost compare to other related schemes. The binary code is the key using here to encrypt and decrypt. Earlier fingerprint, facial recognition, pin number, one-time password and some other processes are used. Binary code as a private key is a most protected way for user's data. For a fingerprint scanning process, when user's finger got injured, the problem will occur to encrypt and decrypt. Like this for every process got some privacy lag. Binary code accessing is the most secure process for any security process. The components used are RFID reader and RFID tag. Radio Frequency identification reader is used to gather information from an RFID tag. It is used to track the individual objects like tags, electromagnetic fields. The tags contain the electronically stored information. The tags are two types one is Passive tags and the other is an Active tag. Passive tags collect energy from a nearby RFID reader that produces the radio waves. Active tags have a local power source like battery and it may operate hundreds of meters from the RFID reader.

![Fig 1: Dual-Factor Authentication System](image)

This RFID technology is similar to the barcodes. The RFID tag can be scanned in any way do not have to be scanned directly or in the line of sight to a reader. The tag must be within the range of 3 to 300 feet to the RFID reader. The tag can be scanned for many times and enables fast identification of a particular product if the RFID reader is surrounded by several items the reader will read the card because the electromagnetic waves are so powerful.
Active RFID and Passive RFID tags are the types of RFID tags. These two types are varied by their owing of power sources. Active RFID tag contains its own power source, often like a battery. Passive RFID tag does not need batteries. From a reading antenna, it gets its power required. These RFID tags identification barcodes cannot be changed because of their cost, each tag has an individual identity for every item.

The RFID technology is used in some applications like Passports, Airplane luggage, Home appliances, Merchandise tags, Telephone and computer networks, Pallet tracking for inventory. RFID tag contains the digital data tracked or easily scanned by the RFID technology. RFID tag is made up of integrated circuits. These contain a tiny antenna for transferring information to an RFID transceiver. The most RFID tags contains an integrated circuit for modulating and demodulating the radio frequency and also an antenna for transmitting and receiving signals. Radiofrequency ranges from low with 125 to 134kHz and 140 to 148.5 kHz, high with 850 to 950 MHz and 2.4 to 2.5GHz. Wavelengths on 2.4 GHz range are very less because they can be absorbed by water. The data in a common RFID tag can be read by anyone easily. User can't be able to know how the data is exposed. This is due to the reason that the RFID tags have a less amount of computing power which is not enough for encryption. In the case of RFID tags used in passports, they have sufficient computer power for the encryption.

There are three pieces of information used in the passport – the passport number, the birth date of the passport holder and passport's expiration date – along with checksum digit for each of the three. This is called Basic Access Control (BAC). The U.S State Department adopted BAC system in 2007 and added an anti-skimming material to electronic passports to reduce the threat of attempts to steal user's personal information.

4. BLOCK DIAGRAM:

The user will first access the smart card if the smart card is accessible otherwise the access will get denied. Using Elliptical Curve Cryptography the binary code will be generated.
The generated binary code will check the accessibility in the database provided. If the matching binary code is available in the database, the locking system will be accessed automatically. Otherwise, the control will go back to the user notifying that the password is invalid.

![Flow Diagram](image1)

Figure 3. Flow Diagram

The user can modify the password anytime. Binary System will be more secure than the related schemes. Tapping system makes user easy for access. The password or any information will be hidden under an image and when some people tried to see the information, only the image will be shown. Security level will be increased by using this scheme.

5. **ALGORITHM**

MD5 Algorithm:

![Algorithm Diagram](image2)

Figure 4. Algorithm
The MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. MD5 is a message-digest algorithm which produces an output of a message of arbitrary length as a 128-bit message. This is used for digital signature applications where compression takes place for a large file. This is a secure manner before being encrypted with a private key. MD5 is one of the most efficient algorithms currently in use.

**Implementation steps:**

**Step 1. Append padding bits**

The input message is "padded" (extended) so that its length (in bits) equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512. Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512. At least one bit and at most 512 bits are appended.

**Step 2. Append length**

A 64-bit representation of the length of the message is appended to the result of step 1. If the length of the message is greater than $2^{64}$, only the low-order 64 bits will be used. The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message will have a length that is an exact multiple of 16 (32-bit) words.

**Step 3. Initialize MD buffer**

A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first):

- word A: 01 23 45 67
- word B: 89 ab cd ef
- word C: fe dc ba 98
- word D: 76 54 32 10

**Step 4. Process message in 16-word blocks**

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

- $F(X, Y, Z) = XYZ$ or not $(X)Z$
- $G(X, Y, Z) = XZ$ or $Y$ not $(Z)$
- $H(X, Y, Z) = X$ xor $Y$ xor $Z$
- $I(X, Y, Z) = Y$ xor $(X$ or not $(Z))$

**Elliptical Curve Cryptography:**

ECC offers greater security for a given key size. The smaller key size also makes possible much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software. There are extremely efficient, compact hardware implementations available for ECC exponentiation operations, offering potential reductions in implementation footprint even beyond those due to the smaller key length alone.
GROUP

A set of objects and an operation on pairs of those objects form which a third object is generated. The group must be closed, invertible, the operation must be associative, and there must be an identity element.

Example: integers 0-9 and addition modulo 10

- Closed: the sum of 2 numbers from 0-9 modulo 10 is an integer from 0 to 9.
- Identity: 0 since 0+x = x for any x
- Invertible: x + (10-x) = 0 mod 10 for any x
  So (10-x) is the inverse of x
- Associative: (x+y)+z = x+(y+z)

Finite Field:

If p is any prime number and n is any positive integer, then there exists a finite field of size p n. There are no other finite fields.

Example: p = 7, n = 1, operation = *

G = \{ g0, g1, g2, g3, g4, g5 \} 0 0 0 0 0 0 0 is a group, then g6 = g0 and 1 0 1 2 3 4 5 6

G is cyclic 2 0 2 4 6 1 3 5 3 0 3 6 2 5 1 4

generator = 3 4 0 4 1 5 2 6 3 3, 2, 6, 4, 5, 1, 3 5 0 5 3 1 6 4 2

inverse: 6 0 6 5 4 3 2 1 1:1, 2:4, 3:5, 4:2, 5:3, 6:6

6. RESULT and DISCUSSIONS:

After entering admin login details, the smart card is to be tapped.

The binary code is generated and one tab is opened for admin to add image and the data that is to be secured.
After adding image and data, the data will be hidden before that Image. The user after login, cannot see the data directly, he can only see the image. After tapping, the data will be displayed.

**Figure 7. Input image**

**Figure 8. Output image**

### 7. Conclusion:

Smart card based authentication scheme has been widely utilized for various transaction-oriented services such as electronic currency exchange, social insurance payment, and e-commerce payment charge in modern society. To develop a smart card based authentication scheme to support initiator traceability and defend against major security threats for a transaction service user has become a crucial topic for researchers. Recent efforts for developing anonymous authentication scheme with the smart card have failed to provide initiator non-tracing ability for a user or be vulnerable to some security attacks.

### References:

[1] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," IEEE Trans. Ind. Inf., vol.9, no. 1, pp. 277-293, 2013.
[2] Mayan, J.A., Priya, K.L.," Novel approach to reuse unused test cases in a GUI based application", IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015,pp.1-7
[3] D. Liu, M. C. Lee, and D. Wu, "A Node-to-Node Location Verification Method," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1526 - 1537, May 2010.
[4] C. Chang and C. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629-637, Jan. 2012.
[5] G. Wang, J. Yu, and Q. Xie, "Security analysis of a single sign-On Mechanism for Distributed Computer Networks," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 294-302, 2013.
[6] L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing," IEEE Trans. Ind. Electron. vol. 58, no. 6, pp. 2163-2172, Oct. 2010.
[7] Albert Mayan J, Anto Praveena M D, Telkar Bharath Rao, Uravakonda Uday Sagar (2018), "Optimized test data generation over suspicious implementation of oracle problem", IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017), pp. 2559-2563.
[8] B. Wang and M. Ma, "A server independent authentication scheme for RFID systems," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689-696, Aug. 2012.
[9] Mayan J.A, Arifa S, Pavithra R,"Semantic based multi lexical ranking technique for an effective search in protected cloud, 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, 2016, pp. 570-576.
[10] Asha P, Albert Mayan J, Canessane A (2018), "Efficient Mining of Positive and Negative Itemsets Using K-Means Clustering to Access the Risk of Cancer Patients", Communications in Computer and Information Science, ICSCS 2018, Kollam, 2018, pp. 373-382.