RFID and Biometric Fingerprint Based 3-Factor Authentication System for High Security Zones

Sanketh Iyer, P.G. Student, Department of Information Technology, PTVA's Mulund College of Commerce, University of Mumbai, Mumbai, India, sanketiyer.217@gmail.com

Dr. Hiren Dand, Coordinator, Department of Information Technology, PTVA's Mulund College of Commerce, University of Mumbai, Mumbai, India, dandhiren@yahoo.co.in

Dr. Rajendra Patil, Department of Information Technology, S.K. Somaiya College, University of Mumbai, Mumbai, India, patilrajendrab@gmail.com

Abstract: Authentication is a process wherein the identity of a genuine user is established. Over the course of time various authentication methods have been used which have their own pros and cons. The most basic method of authentication was knowing a secret word called the password. However, the secret word could be known by anybody and hence a checker mechanism was put into place where there would be a username and a password and each user can keep his own unique password. Again, the problem was encountered when this username and password could be compromised and be used by any person posing to be the genuine user. Then came the two-factor authentication mechanism where the identity of the user would also be established. With enhancements in technology, RFID cards and biometric devices have become a very common tool for authentication due to their cheap rate and simplicity in many organizations. Their working and implementation are also fairly simple. In this paper, going a level further we would discuss the implementation of a 3-factor authentication system using these RFID cards and biometric fingerprint reader.

Keywords: Authentication, Biometrics, Encryption, RFID Card, Security, Skimming, Spoofing.

I. INTRODUCTION

RFID Cards have become a fairly common method of authentication in most of the organizations. The simplest one we can recollect anytime is that the user simply hovers his card over a small module and the door opens. This means that the user is authorized to enter the department or section of the organization. However, RFID cards have their own drawbacks that we will be discussing in the latter section of the paper. This simplicity of using RFID cards have prompted many organizations to adapt RFID based authentication systems. However, the biggest security loophole of an RFID system is because of the RFID skimming. This renders the entire RFID based authentication useless.

A biometric fingerprint reader can be seen in almost every organization, popularly used as an access control and attendance system. The fingerprint reader has a reputation of being extremely strong authentication device just because no one can manipulate the fingerprint of the living person. But there are rare circumstances wherein a fingerprint device can also fail due to spoofing or data leak attacks. If the biometric database of a system is compromised then the fingerprint data of a person can be obtained which can be spoofed. Therefore, again somewhere this system is also not completely trustworthy.

Authentication is when the identity of a person or user is established. Various authentication methods have been established wherein the most common one these days being Username and Password. The Username becomes a unique ID which can be granted to a specific user by the administrators or can be custom made by the user. This username can be only a set of numbers as an ID, a set of characters e.g. a name, or a combination of both along with a permitted set of special characters. Passwords are secret words that are stored along with the username in the database. These passwords have to be strong and are usually a combination of Alphabets, numeric and a permitted set of special characters. For successful authentication to take place the username and passwords must match, and on successful match access is granted to the user. This is the general authentication found on most of the systems and is famously referred to as the 1-Factor Authentication. However, this is prone to brute force attacks, which means if an adversary can get hold of the username then he can brute force the password by guessing it, running a dictionary over it or using and advanced

 DOI : 10.18231/2454-9150.2018.1390

algorithm to try multiple combinations of characters and numeric along with special characters.

Considering the security scenario and the advancements made by hackers in breaking the rapidly growing technology, multifactor authentications were put into place. These multi-factor authentications used some methods to identify the user in order to grant access. They could easily provide and additional layer of security along with the traditional 1-Factor Authentication layer. In this paper we would try to demonstrate an effective 3-Factor authentication method using RFID cards and Biometric fingerprint that would provide an unchallenged level of security to any organization implementing it.

II. THREE FACTORS OF AUTHENTICATION

We have been continuously using the term "Factors of Authentication" along with a number. These Factors of authentication are universally accepted principles that are applied before creating any authentication mechanism. The three factors of authentication are as follows [5], [7]: -

- Something what you know (such as a username and password)
- Something what you have (Such as an RFID card)
- Something what you are (Such as one's biometric authentication)

We would be implementing three of these in our proposed authentication.

III. ALL ABOUT RFID

RFID stands for Radio Frequency Identification [1]. They are closely related to smart cards which are also popularly used. Data in RFID cards are stored in electronic form called the transponder. However, the major difference between smart card and the RFID is that data transfer / or data reading occurs in the form of non-galvanic contacts i.e. using electromagnetic fields [2]. This gives the user a feather touch feel and comfort as he need not insert or swipe a card but simply needs to hover or touch the card on a device.

The entire RFID system is made up of two components [3]: -

(a) The transponder, which is embedded in the RFID card.

(b) The interrogator or reader which is connected with a system which can process the information which is received from the transponder by the reader.

An RFID card can typically store between 16-64k bytes. This is enough for it to store simple identity information. Data reading capability is very fast typically less than 0.5 m.s. Recently RFID was known to be prone to the RFID Skimming and Cloning attacks.

Skimming is fairly simple and can be achieved by any simple RFID card reader. If the information stored on the RFID is in plaintext then any adversary can simply read it using a handheld RFID reader. Cloning is fairly difficult to achieve considering the UID an RFID card has however is not difficult as well. The RFID tag can replicate its UID in exact form factor [4]. All this is stemmed by the fact that to communicate with an RFID and as it communicates simply over RF, there is no authentication that is required.

IV. BIOMETRIC FINGERPRINT AUTHENTICATION

Biometric fingerprint authentications are one of the strongest known authentication mechanisms that's available in the market [6]. This is supported by a standalone biometric system that would locally store the biometric data of the authorized users or it can be a reader which is connected to a back-end software or a centralized server.

As said earlier, biometric is known to be a very mature technique having very few flaws that are known [8], however in the security world, nothing is known to be flawless and there are unknown adversaries who are continuously working in order to break the emerging technologies and gain advantages over it.

The Biometric fingerprint-based authentication system is very popular in the finance sector, especially in the banking industry [9] where security is of utmost importance. These days ATM's are being loaded with biometric authentication systems which would provide an additional layer of security [6].

Insecure storage of biometric data or vulnerabilities in the biometric system may allow the hacker to access the biometric database and clone unique fingerprints. Vulnerable components in the biometric system may lead to a hacker compromising the system and rendering it useless. The fingerprint data can be faked using artificial cloning methods in order to bypass the biometric authentication system.

V. THE PROPOSED SYSTEM

The proposed system would be a standalone system that would provide an interactive UI on a display screen, having an interrogator interface for reading RFID cards and a biometric fingerprint reader interface. The below flowchart shows step by step instruction on how the system would be working. A detailed discussion on the same would be given below.

The entire process has been divided into 4 steps, the 4th one being the grant of access. In case of any failures, the user has to begin all the way again. The Processes and sub-processes involved are as follows:-

1. The user scans the RFID card
   A. The RFID Authentication process begins

 DOI : 10.18231/2454-9150.2018.1390

B. The process checks the database for RFID data and either a positive or negative response is received.

C. In case of a negative response the process is terminated with a "Not Authorized" Message.

D. In case of a positive response, the process moves to step 2.

2. The biometric stage begins wherein the use scans his finger as a biometric authentication.
   A. The biometric authentication process is triggered.
   B. The process checks the database for relevant biometric data and either a positive or negative response is triggered.
   C. In case of a negative response the process is terminated with a "Not Authorized" Message.
   D. In case of a positive response, the process moves to step 3.
3. The last and final step is wherein the machine asks for a PIN. This is the password stage.
   A. The PIN based authentication process is triggered.
   B. The process checks the database for correct PIN and either a positive or negative response is triggered.
   C. In case of a negative response the process is terminated with a "Not Authorized" Message.
   D. In case of a positive response, the process moves to step 4 and Access is granted.
4. The Last step here is the grant of access to the fully authenticated user.

As we see in the above steps, a 3-Factor Authentication mechanism is established as follows:

(a) In Step 1 we scan the RFID - Something what we have
(b) In step 2 we scan the fingerprint – Something what we are
(c) In step 3 we input the PIN – Something what we know.

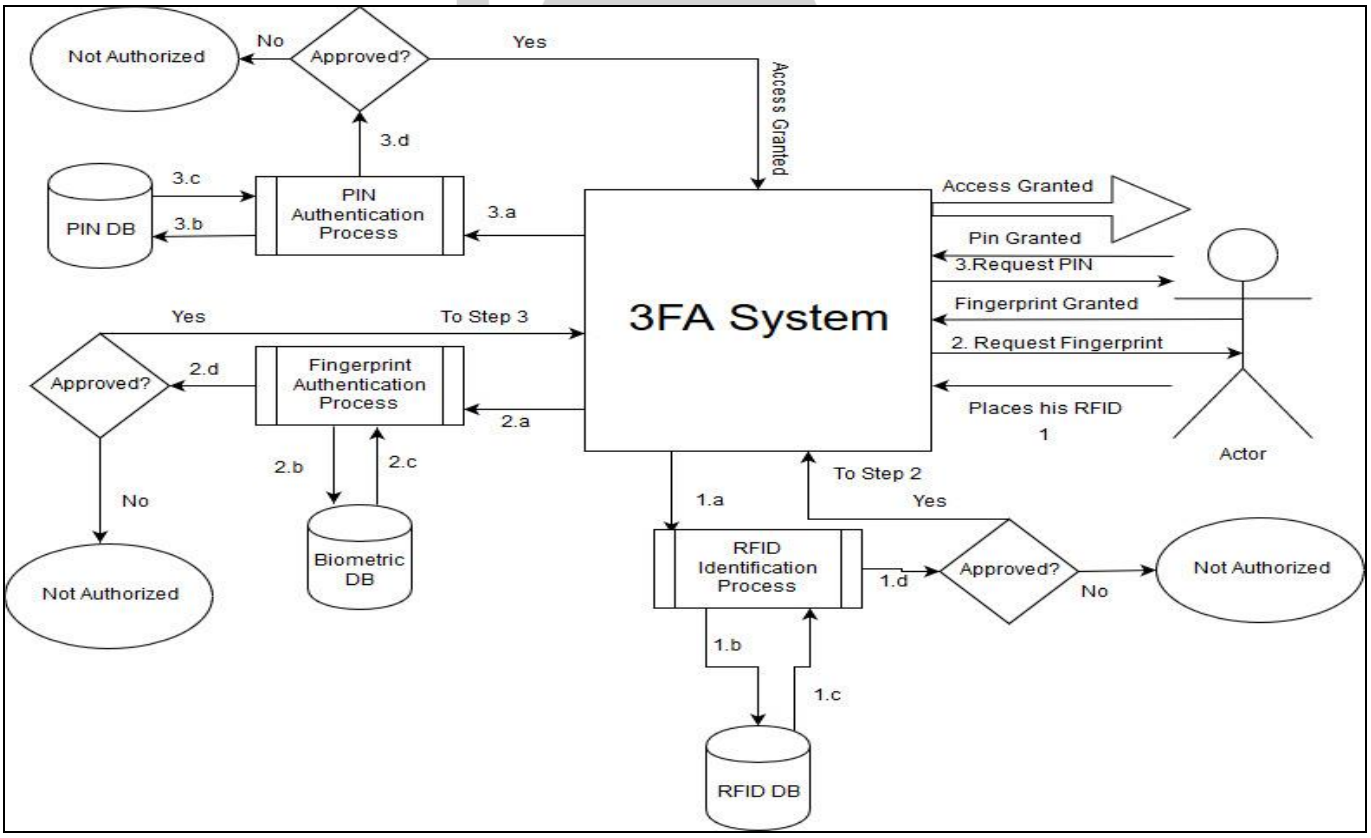

Figure 1: Entire working flow of the proposed system

The entire system demonstrated above prompts the user three times as discussed in the order above. The last prompt of the authentication process is the PIN based authentication step. This can be achieved either using a static PIN or a dynamic pin generated either through an authentication token or through Mobile OTP [10]. The dynamic PIN can be generated using the mobile phone as an authentication token using an application that generates PIN using a predetermined algorithm. The static PIN can be generated once and can be memorized by the user for any future transactions. The entire process is presumed to be very fast as the authentication uses known and efficient methods. The RFID and biometric fingerprint-based authentications are known to have very less overhead. The only sticky area maybe the PIN based authentication wherein generation of PIN or OTP may take time. However, if we go for the static PIN method then its purely the time taken for user to input the PIN. The complete

 DOI : 10.18231/2454-9150.2018.1390

performance shall also be influenced by database access time and network efficiency of the entire system. If the system can be implemented as a standalone embedded system, then the efficiency of the entire system can be improved a lot. As said earlier, the three factors of authentication here provide a strong security and acts a deterrent to prevent any breach.

VI. THE ADVANTAGES OF THIS SYSTEM

The system would be foul proof especially due to the presence of biometric fingerprint-based authentication. Spoofing a fingerprint or biometric would seem easy but it's not practically feasible for any adversary. Furthermore, the entire authentication proceeds stepwise and a failure at any step requires the user to start again. The information stored on the RFID card as well as the databases behind would be completely encrypted with the best encryption standards. The PIN would be regularly subject to change as per the organizations policy. The entire system is designed to safeguard access to High security Zones which indeed is not accessible to many users. RFID and fingerprint based biometric authentication are known to be fast and efficient therefore it may not compromise functional or ease of use in any way. The ultimate factor is the trust that the organizations can place in this system as three components of this system are known to be foul-proof and some additional physical security can be placed in order to prevent any security gaps.

VII. CONCLUSION

Multifactor authentications have been generally deemed to be secure compared to single factor authentication. As demonstrated above, the system implements three factors of authentication. The RFID system fulfils "What you have"

, the biometric system fulfils "What you are" and finally the Password system fulfils "What you know" hereby completing the triangle of three factor authentication. Compromising all the three factors of authentication is unheard of. The first strength of this system is because the compromise of biometrics is a very distant possibility as biometric information is not that easily manipulative. The second strength is RFID, which can be easily disabled on immediate reported loss and can be safeguarded by the user. This makes the PIN system appear only like an additional addon, but yes, this additional security is also an added advantage during a rare scenario of the other two getting compromised. All this provides an extended strength to this system. With advancements in security, hackers are also becoming advanced in their techniques to crack security infrastructure and reap the benefits of the Hack Value. Therefore, security researchers prefer to implement multi layered security architectures in order to contain any breach at the lowest levels. By multi layering security and interconnecting them, Hackers find it more difficult to breach each and every layer and if such breach occurs in one layer, it is detected and immediately patched before any advancements can be made. Therefore, it is recommended to go for multi factored authentication systems in order to achieve maximum security. This also goes with the concept that complicating the security would indirectly strengthen it. The above system tries to achieve the same by using the latest technology along with affordable components.

REFERENCES

[1] Finkenzeller, K.,RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication,John Wiley & Sons,p4-p6,2010

[2] Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. S., RFID technology principles, advantages, limitations & its applications., International Journal of Computer and Electrical Engineering,ISSN: 1793-8163,Vol. 3,No. 1, 153-154,2011.

[3] Ravi, K. S., Varun, G. H., Vamsi, T., & Pratyusha, P., RFID based security system. International Journal of Innovative Technology and Exploring Engineering,ISSN:2278-3075,Vol. 2,No. 5, 132-134,2013

[4] Weber, C., Saiyed, A., Kamani, M., & Sivalingam, P. RFID Skimming and Cloning Attacks on Presto Cards.p3

[5] Choi, S., & Zage, D.,Addressing insider threat using "where you are" as fourth factor authentication In Security Technology (ICCST), 2012 IEEE International Carnahan Conference on.,pp.147-148,2012.

[6] Das, S., & Debbarma, J., Designing a biometric strategy (fingerprint) measure for enhancing atm security in indian e-banking system. International Journal of Information and Communication Technology Research,Vol. 1,No. 5,.pp197-199,2011

[7] Kim, Jae-Jung, and Seng-Phil Hong. A method of risk assessment for multi-factor authentication. Journal of Information Processing Systems,Vol, 7, No.1,pp187-198,2011

[8] Wayman, J., Jain, A., Maltoni, D., & Maio, D. ,An introduction to biometric authentication systems. In Biometric Systems, Springer, London. 1-20,2005.

[9] Bhattacharyya, Debnath, Rahul Ranjan, Farkhod Alisherov, and Minkyu Choi.,Biometric authentication: A review.International Journal of u- and e-Service, Science and Technology,Vol. 2, No. 3 ,pp13-14,2009

[10] Aloul, F., Zahidi, S., & El-Hajj, W. ,Multi factor authentication using mobile phones. International Journal of Mathematics and Computer Science, Vol.4,No.2,pp69-70,2009.

 DOI : 10.18231/2454-9150.2018.1390