ISSN:2348-2079

Volume-10 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

INTEGRATED SECURITY BASED ATM ROBBERY PREVENTION USING RANDOM PIN GENERATION

K. Santhosh, Dr. S. Manju Priya*

Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India
Professor, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.

Corresponding Author: Dr. S. Manju Priya
Email: manjupriyacs@kahedu.edu.in

ABSTRACT

The automated teller computing device is used to withdraw cash at any time somewhere in the world. Automated Teller Machine (ATM) is a mechanized raconteur machine that is an automated gadget that serves the media in transmissions in which a monetary entity provides consumers with access to budgetary alternatives in a free space without a human assistant or bank worker's involvement. This study of focused on design and implementation of face detection based ATM security system using embedded Linux platform. High level security mechanism is provided by the consecutive action such as initially system captures the human face and check whether the human face is detected properly or not. ATM-based networking options furnish one feasible choice to assembly these overall performance needs. Future ATM, and its related infrastructure, provide incredible viable for growing the effectivity of operations and for security enhancement on a world scale, while in the longer time period decreasing charges typical to the advantage of all stakeholders. Authentication is the initial stage of protection towards compromising confidentiality and integrity. Though typical login/password-based schemes are effortless to implement, they have been exposed to innumerable attacks. As an alternative, token and biometric based totally authentication structures had been introduced. However, they have now not elevated notably to justify the investment. Thus, a variant to the login/password scheme, viz. OTP scheme with interchanging the 2nd and 4th letter of pin variety with the aid of receiving the OTP. But it furthermore suffered due to shoulder-surfing and display screen dump attacks. If an attacker manages to get maintain of ATM card and the pin wide variety might also effortlessly use it to withdraw cash frequently. Thus this device gives a absolutely tightly closed way to function ATM transaction with protection structures.

Keywords: ATM, OTP, Security, HMAC

I. INTRODUCTION

The Internet is a vital phase of our day by day life, and the share of peoples who assume to be in a position to control their financial institution money owed anywhere, whenever is continuously increased [2]. As such, Internet banking has come as a quintessential element of any monetary institutions. Online banking is one of the touchiest duties carried out with the aid of familiar net user. Security of a customer's economic facts is very important, besides which on line banking couldn't be successful. Financial establishments have set up a variety of protection strategies to limit the danger of unauthorized on-line get right of entry to a customer's records, however there is now not a single one approach that fulfills all the requirements. Most of the assaults on on-line banking used nowadays are primarily based on steal person login statistics and legitimate TANs.

Though normal login/password primarily based schemes are handy to implement, they have been subjected to quite a few attacks. As an alternative, token and biometric based totally authentication structures had been introduced. However, they have no longer expanded notably to justify the investment.

Thus, a version to the present scheme, viz. OTP scheme with interchanging the 2nd and 4th letter of pin variety through receiving the OTP is used.

If an attacker manages to get keep of ATM card and the pin wide variety may additionally without difficulty use it to withdraw cash frequently. Thus our gadget offers a completely impenetrable way to function ATM transaction with safety structures.

II. EXISTING SYSTEM

The traditional username/password or PIN based authentication scheme is an example of the "what you know type". Smartcards. As a substitute to the traditional password-based scheme, the biometric system was familiarized. This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc.

Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose [1]**.** The growth in electronic transactions and banking system has resulted in greater demand for fast access of banking transactions with the aid of Automated Teller Machine (ATM). The quick increment in the utilization of ATM transactions has been closely followed by the increase in ATM frauds. OTP techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text [6].

Disadvantages

- Alphanumeric passwords are used widely, they have troubles such as being difficult to remember, prone to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering.
- The most important hassle of biometric as an authentication scheme is the excessive fee of extra gadgets wanted for identification process [9]. This is misuse of memory and late response to emergency condition. In this manner, early disclosure of the condition is essential to take preventive measures against a non-stop robbery.
- Although password appears to be handy to remember, which will increase the usability, it is now not definitely secure. It wishes a number of rounds of authentication to grant a fairly massive password space, which is tedious.

III. PROPOSED SYSTEM

Our proposed system will provide advanced ATM theft security system. The afflatus for our project is gained from the news and issues which are happening in our daily life [5]. Now a day's larceny or robbery of ATM is superabundantly increased so due to that we trying to disclose remedy [7]. This project gives the alert at the instant of time when the thief is about to break the ATM machine. So, to overcome the drawbacks in the existing systems in our society. Whenever the thief is bringing the tools for the robbery into the ATM or when the thief is trying to use the tool to break, the CCTV camera on the ATM sense whether the person is bringing tools using the deep learning techniques and machine learning. In the proposed machine OTP scheme with interchanging the 2nd and 4th letter of pin wide variety through receiving the OTP. But it additionally suffered due to shoulder-surfing and display dump attacks. If an attacker manages to get maintain of ATM card and the pin wide variety might also effortlessly use it to withdraw cash frequently. Thus, our gadget offers a absolutely impervious way to operate ATM transaction with safety structures.

Advantages

- The power of OTP relies upon appreciably on how correctly the authentication data is embedded implicitly and it must be convenient to be mindful for a legit consumer and pretty fuzzy for a non-legitimate user.
- The gadget offers higher safety in opposition to dictionary and brute force attacks as password modifications for each and every session [4].

A wide variety of systems need reliable personal recognition system to either authorize or determine the identity of an individual demanding their services. The goal of such system is to warrant that the rendered services are accessed only by a genuine user and no one else [8]. This system consist different sensors to continuously monitor its surrounding for suspicious activities like physical attack, break in and theft might jeopardize the ATM and people nearby the machine. In the absence of robust personal recognition schemes, these systems are vulnerable to the deceits of an imposter.

Algorithm /Methodology

In cryptography, a HMAC is a particular sort of message verification code (Macintosh) including a cryptographic hash work and a mystery cryptographic key. To confirm at the same time both the information trustworthiness and the legitimacy of a message, HMAC 256 was utilized. To ascertain HMAC; cryptographic hash work, for example, SHA-256 or SHA-3, might be utilized in the subsequent Macintosh calculation is named HMAC- X, where X is the hash work. Cryptographic quality of the basic hash work decides the cryptographic quality of the HMAC.

HMAC uses two passes of hash computation. The two keys can be derived from secret keys – internal and outer. An interior hash derived from the message and the inner key in the first pass of the algorithm. The closing HMAC code derived from the inner hashend result and the outer key are the second skip of thealgorithm. When in contrast to length extension attacks, this algorithm gives higher immunity. Two paddings are used here, that are ipad and opad.

The message broke down into blocks of a constant size with the aid of iterative hash feature and compression function iterates over them.

The message will not be encrypted by way of HMAC. Instead, the message (encrypted or not) should be dispatched alongside the HMAC hash. Parties with the secret key will hash the messageonce more themselves, and if it is authentic, the obtained and computed hashes will match. two Mihir Bellare, Ran Canetti, and Hugo Krawczyk, posted definition and analysis of the HMAC building in 1996 and in 1997 they also wrote RFC 2104. Generalized and standardized the use of HMACs by means of FIPS PUB 198. IPsec and TLS protocols make use of HMAC and additionally HMAC was used inside the JSON Web Tokens

$$\text{HMAC}(K, M) = H((\acute{k} \pm \text{Opad}) \| H((\acute{k} \pm \text{ipad}) \| m)) \quad (1)$$

$$\acute{k} = H(K) \text{ k is larger than block size} \quad (2).$$

Security

The cryptographic electricity about the HMAC depends a top over the dosage concerning the unseen resolution so much is used. The most frequent onfall closer to HMACs is animal pressure in imitation of find the stolen key. HMACs are significantly a good deal much less affected by way of using collisions than theirs underlying hashing algorithms alone. In particular, of 2006 Mihir Bellare ascertained up to expectation HMAC is a PRF beneath the mere grant that the suppression characteristic is a PRF. Therefore, HMAC-MD5 does in modern times not gothrough out of the equal weaknesses so much have been performed into MD5.

HMAC (k,m) is computed as HMAC(H(k), m)when the key is longer than the hash block dimension where keys longer than B bytes are hashed the use of H" which leads to a problematic pseudo-collision required by way of way of RFC2104.This leads to thesusceptible spot of HMAC in password-hashing scenarios: it describes that the values will produce theidentical HMAC output when feasible to locate along ASCII string and a random price whose hash will be also an ASCII string.

To distinguish HMAC with reduced variations of MD5 and SHA-1 or full versions of HAVAL, MD4, and SHA-0 from a random characteristic or HMAC with a random characteristic showed via Jong sung Kim, Alex Belyakov, Bart Pernell and Seokhie in 2006 . Differential distinguishers permit an attackerto devise a forgery attack on HMAC. Furthermore, second-preimage attacks were due to rectangle distinguishers and differential. HMAC with the full version of MD4 can be forged with this knowledge. The security proof of HMAC was once now not contradicted with these attacks, but grant insight into HMAC based totally on present cryptographic hash functions [3]. Automated teller machine (ATM) nowadays are a favourite spot for attackers as they are available everywhere and are much easier to rob. Generally, ATM attacks can be either physical ATM attacks or ATM-related fraud attacks. In this paper the idea of an ATM system with multilayer security is proposed with the help of internet of things (IoT), fingerprint identification and face recognition to increase the security of ATM.

In 2009, Xiao Yun Wang et al described a distinguishing attack regarding HMAC-MD5 outside of the use of associated keys. It be able separate an instantiation concerning HMAC together with MD5 out of an instantiation with a random function with 297 queries together with gamble 0.87.

IV. RESULT AND SCREENSHOTS

1. Admin login

Admin login used login in authenticate admin user

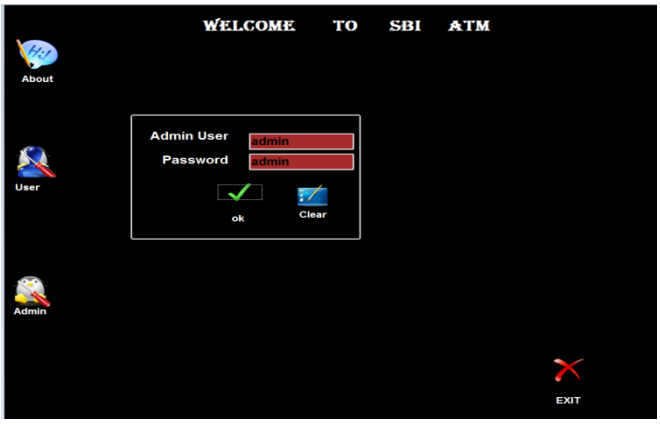

Fig 1: Admin login

2. User registration

New user register to accessing the Application

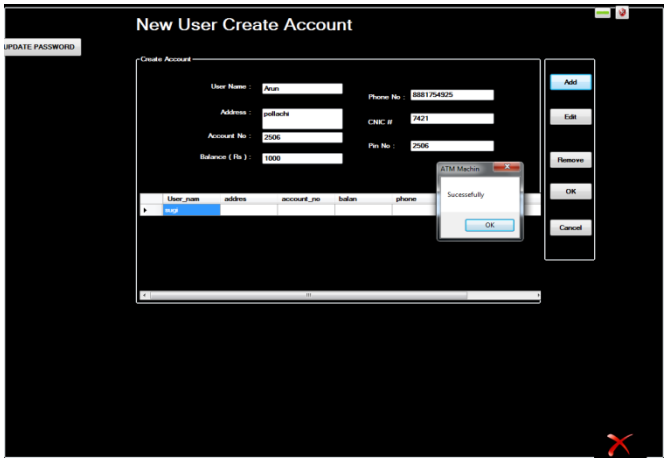

Fig 2: User registration

3. Key generation

Key Generation Scheme used to generate access key

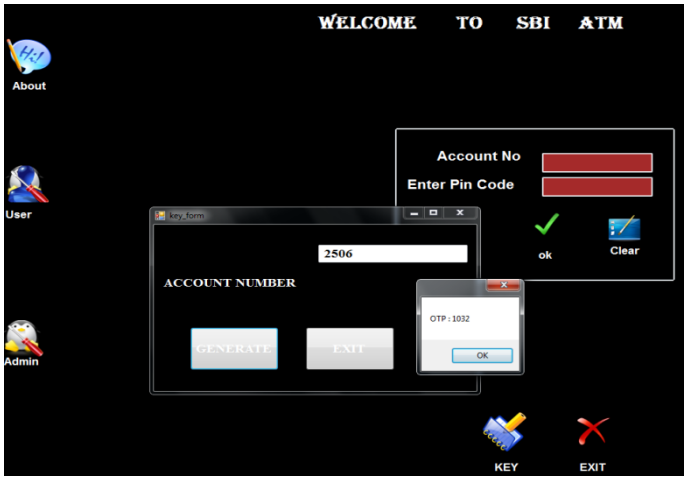

Fig 3: Key generation

4. Deposit

Deposit form used to deposit the cash in bank

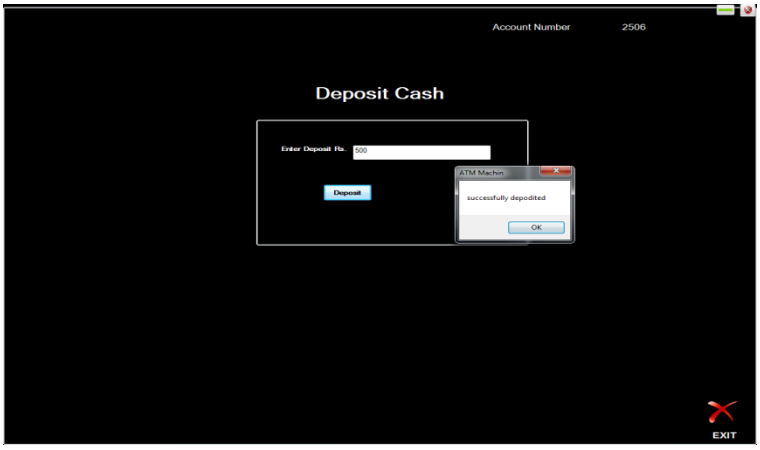

Fig 4: Deposit

5. Withdraw

Withdrawn form used to withdrawn cash from bank

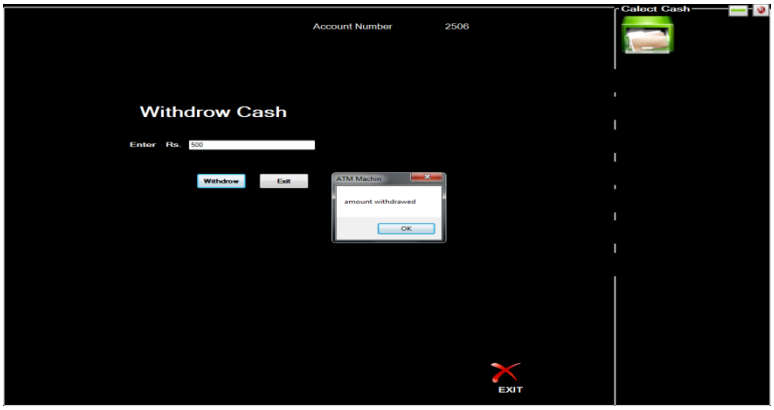

Fig 5: Withdraw

6. Balance

Balance form is used to knowing the account balance

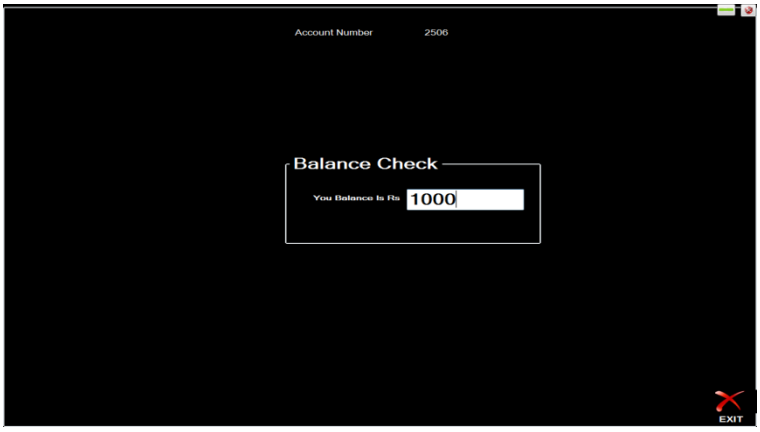

Fig 6: Balance

V. CONCLUSION

In this paper, a framework and the working model of the software is provided which gives integrated security that ensure avoiding ATM robberies. The adopted technology is cheaper to deployed. In general, it can positively impact the banking industry and society by reducing the ATM theft.

REFERENCES

1. Druva Kumar S, Ravindra, Hosamani SB, Kiran Y, Manju SN. Atm robbery prevention using advanced Security system. Int J Emerg Technol Innov Res;5(5), page no.491-493.
2. Krishna Prasad K. A study on multi phase Security solutions to ATM banking systems. Int J Appl Eng Manag Lett. 2018;2(2, November).
3. Mehta G. A review paper on ATM Security. J Emerg Technol Innov Res, Volume 5 Issue 2. February 2018.
4. Joy A, Babu C. Design and implementation of multilayer Security for ATM machines. Int J Recent Technol Eng. 2021;10(2, July):39-43. doi: 10.35940/ijrte.B6112.0710221.
5. Twum F, Nti K, Asante M. Improving Security levels in automatic teller machines (ATM) using multifactor authentication. Int J Sci Eng Appl. 2016;5(3):126-34. doi: 10.7753/IJSEA0503.1003.
6. Lignesh J. Patoliya ”Face Detection based ATM Security System using Embedded Linux Platform”, 2nd International Conference for Convergence in Technology (I2CT); 2017.
7. Kumaresan R, Dharanidharan GV, Gomathi S. ATM-Robbery prevention using machine learning technique. Int J Adv Res Ideas Innovative. Technology Publishing, 2019.
8. Kambale Ms VH. Atm crime prevention system. Asian J Converg Technol (AJCT). 2018:ISSN-2350-1146.
9. Padman K, Shetty S, Rai A, Grace B. Smart video surveillance for ATM. Alvas Inst Eng Technol.ISSN-0039-2049. 2019;6(6).