Enhancing Authentication Methods in Online Banking Using Face Recognition with Hybrid Pins

Abstract: Researchers have been drawn to this problem because of the increasing prevalence of authentication-related malware and the critical nature of authentication security. Since the current password-based authentication paradigms are inefficient, not robust enough, and susceptible to automated attacks, many such attacks succeed in gaining access to social network accounts. Alternatively, two-factor authentication (using a combination of a password and another piece of information, like a one-time PIN issued by the user's device or an SMS) can be used to bolster the security of single-factor authentication. This study presents a novel approach to preventing shoulder-surfing attacks on authentication systems by employing a three-layer-based authentication system. The first tier uses biometric authentication to solve security and privacy concerns in novel ways. The goal of incorporating face biometrics into a real-time authentication system is to ensure that only authorised users may access ATMs. OTP verification using reverse processing is provided at the second layer of security. Then, have a PIN-based authentication system in place that can be used with ATM software. A hybrid keypad is a keypad that employs the concept of merging two keypads with distinct digit orderings in such a way that the user, when up close to the device, sees one keypad to enter the PIN, but an attacker, when looking at the device from a further distance, sees only the other keypad. Upon entering their credentials, users activate the application's three-factor authentication process.

Key words: Enhancing Authentication, Methods, Online Banking, Face Recognition, Hybrid Pins.

Introduction

Network security refers to the measures used to protect against and detect attacks on a network and the data and programmes available over it [8]. The administrator of a network is responsible for deciding who is allowed access to the network's data [9]. Users gain access to resources within their purview via a user ID and password (or other authenticating credentials) that they select (or are assigned) [10]. Public
and private computer networks are both included in the scope of network security since they are essential for the smooth operation of modern corporations, government institutions, and private households. Some networks are only accessible within a certain organisation, while others are available to the whole public [11]. Organizations, businesses, and other establishments all have a hand in network security. As its name implies, it ensures the safety of the network and keeps an eye on all the goings-on within it. Network resources are often protected through the application of a name and password [12].

Authentication, typically in the form of a username and password, is the first step in ensuring a safe network. One-factor authentication is frequently used to describe this method because it only requires one piece of information (the password) to verify the user's identity. Three-factor authentication requires not just something the user knows (password) but also something the user "possesses" (a security token or "dongle," an ATM card, or a mobile phone) [13-15].

Firewalls are used to control who may access certain parts of a network and what services they can utilise after they have been granted access. While this feature is great at stopping hackers, it may miss anything more serious like computer worms or Trojan horses that are being communicated across the network. Malware like this can be detected and stopped with the use of anti-virus software or an intrusion prevention system (IPS) [16-19]. Wire shark-like network monitoring by an anomaly-based intrusion detection system could be logged for auditing and eventual high-level analysis. By analysing all network traffic, modern systems are able to identify active network attackers, whether they are hostile insiders or targeted foreign attackers who have infiltrated a user's workstation or account. It is possible to encrypt network traffic between two hosts for secret communication [20].

Network honeypots, which are essentially decoy resources available through the network, can be used for monitoring and early warning because they are rarely used for their intended purposes. In order to keep tabs on emerging exploitation methods, researchers analyse the methods employed by attackers during and after an assault to compromise these dummy resources [21-23]. The honeypot's protected network could benefit from additional security enhancements if such data were analysed. Additionally, a honeypot can divert an attacker's focus from protected hosts. A honeypot is a fake server set up to divert an attacker's attention away from the genuine server and its data. A honeynet is an intentionally vulnerable network, similar to a honeypot. It's designed to entice attacks so researchers can analyse malicious tactics and improve network defences. One or more honeypots are normally part of a honeynet [24].

**Objectives**

Since secure authentication cannot be judged just based on username and password—since attackers may guess them so easily—this project aims to strengthen the security of Internet Banking through the use of face biometrics and various PIN authentication methods [25]. Financial institutions and their customers alike place a premium on ensuring the safety of online banking. The banking industry has been the target of an alarming number of cyberattacks and acts of fraud in recent years [26-31]. One of the main causes of such accidents is insufficient security processes, especially in regards to authentication. Usernames and passwords are no longer sufficient forms of authentication to prevent modern assaults like phishing, social engineering, and brute force [32].

**Scope of the Project**

The goal of this project is to create and deploy a biometrically-verified and PIN-shuffled authentication system for use with online banking. The goal of the project is to provide an alternative to the conventional means of authentication such as user name and password, which have become increasingly vulnerable due to the proliferation of cyber threats such as phishing. An extra safeguard against theft and fraud can be achieved by the combination of biometric verification and PIN shuffling methods [33]. In order to verify the user's identity, the biometric verification feature will analyse unique characteristics about them, such as their face or voice. User biometric information will be collected at account creation and will be used for further login verification [34]. Because biometric data is specific to each individual,
it is very difficult to copy or falsify, making this technology extremely safe. With the PIN shuffling feature, a new random sequence of digits will be created for each login attempt, thus strengthening the security of the authentication procedure. Even if an attacker obtains the PIN, they will be unable to access the account without the user's permission. The technique will drastically lessen the likelihood of brute-force assaults or guessing the user's PIN by randomly rearranging the PIN each time [35].

Project Goals
The goal of this project is to create and deploy a biometrically-verified and PIN-shuffled authentication system for use with online banking. The system's stated goal is to create a safe, user-friendly, and efficient means of identification that drastically cuts down on the potential for fraud and unwarranted account access in the realm of online banking [36-41]. The goal of the research is to increase safety by combining biometric authentication with PIN shuffling. Facial recognition, fingerprint scanning, and voiceprint analysis are all examples of biometric verification technologies. The system's vulnerability to impersonation and other forms of fraud, such as social engineering and phishing, will be much diminished once this method is put into place. The purpose of the PIN shuffling method is to make it more difficult for an attacker to figure out a user's PIN by producing a new set of digits for each login [42-45]. This method will keep the system safe from intruders by foiling guessing and brute-force attacks. In order to better protect financial transactions conducted online, this initiative will put the system to the test [46].

Literature Survey
The long-term objective of the IoT is to supply services everywhere. There are still numerous obstacles to overcome before this may be accomplished [1]. This paper proposes a bio-inspired self-learning coevolutionary algorithm (BSCA) for dynamic multiobjective optimization of Internet of Things (IoT) services to cut down on energy consumption and service time, which is inspired by the cooperative mechanisms between multiple systems in the human body. The BSCA has three distinct levels. The first level is made up of cooperating subpopulations developing to produce a variety of Pareto fronts. The second layer builds on the first by attempting to generate an even wider variety of solutions from those generated by the first layer. The third layer takes the answers identified in the second layer and refines them using a dynamic optimization approach and an adaptive gradient refinement search strategy to deal with the dynamic nature of concurrent multiple service requests. Based on two service-providing methodologies, i.e., single service and collaborative service, experiments are conducted on agricultural IoT services in the presence of dynamic requests under varied distributions. Specifically for high-dimensional situations, BSCA outperforms four existing IoT service algorithms, as shown by the simulation findings. In order to dynamically optimise IoT services for both cost and time efficiency, this research introduces a bio-inspired self-learning coevolutionary algorithm (BSCA) with a three-layer progressive structure.

In this research, we combine the best features of the three basic authentication types—PINs, cards, and keystroke dynamics [2]—to create a hybrid authentication framework for ATMs that is both secure and efficient. There's no denying that PIN-based verification isn't as effective at keeping your money and identity safe. Their administration and security are becoming increasingly problematic, and there are an infinite number of methods in which they might be stolen, broken, reset, or bypassed by malevolent actors. PIN-based authentication solutions are also advantageous since they reduce the window of opportunity for attackers to guess a valid PIN. The scientists provided additional detail on the nature, distribution, and safety of PINs selected by humans. Internet banking is vulnerable to insecure PIN-based authentication assaults, which can discourage customers from using the service. Several methods are used to fortify these authentication protocols. The usage of a PIN as part of a two-factor authentication system is widespread.

Therefore, we intend to design a system that, in addition to the PIN, also identifies the essence of the person using the card [4]. Clients won't be allowed to proceed to the next page if their photos don't match
those in the database. No entry will be granted, and the cardholder will not be able to make any modifications to their account. The card can be used by the client as well as their allowed companions and children whose information is stored in the database. Therefore, the management of a single card within the household is sufficient, as it will not compromise the safety of the system as a whole. To ensure complete safety, only the most trusted individuals on file will be able to access and use the card. By using this technique, criminals and illegal users are prevented from using ATMs. ATMs utilise face recognition technology in addition to the PIN and OTP for authentication. An actual access card, personal identification number, and facial recognition software would all be part of this machine security approach.

In paper [5], the authors follow the Euclidean distance between the two linked finger codes to complete the unique mark acknowledgment with curvelet variation. The database contains the complete finger codes, and the test finger code is compared to them. If the information provided is a match, a one-time password (OTP) will be given to the user's verified mobile number. The data is preprocessed with the help of the math lab's in-house routines. By slightly adjusting the intensity distribution on a histogram, the histogram equalisation approach aids in working on the global difference of a picture. This makes it possible for regions with poor local contrast to improve their distinctiveness without affecting the global contrast. To do this, histogram adjustment effectively spreads out the most successive power values. Using curvelet transform and fast Fourier transform should allow for component extraction. Adding a GSM module that generates OTP on paper increases the ATM's security. When the GSM infrastructure fails, this system substitutes a Bluetooth connection to the ATM, which generates an OTP reference on the client's mobile device.

This work offers a user-credential-based OTP generation technique for use in a Cloud-based electronic healthcare system in order to safeguard patient information [6]. Since this is an issue, the suggested system employs the proposed secure method to provide the end-user with a secure OTP through SMS (SMS). The proposed solution also offers a safe method of sharing information among the shifting crew via cloud computing. With a group signature, data in the cloud can be shared by any user. For safe information exchange, a group signature is created using individual user credentials. Anyone who wants to join the group must first provide their credentials to the manager. The group manager will authenticate the user's credentials and then offer the group signature to the user so they may access and share data in the cloud. The computational expense of the proposed approach is independent of the total number of suspended users. The cloud's resource management system, load balancing capabilities, and adaptability to user needs are all advantages. It's more than just a trove of digital assets. The price of technology is dropping quickly, while computational power and storage space are expanding dramatically.

System Analysis
The widespread adoption of smartphones has resulted in the storage of a great deal of personally identifiable information. User authentication mechanisms are required to prevent the leak of such sensitive data [47-51]. Shoulder surfing and smudge attacks can compromise current user authentication techniques relying on passwords and patterns. Stroke/gait-based methods, on the other hand, are secure but cumbersome to input. In this work, we present ShakeIn, a user authentication technique that uses the motion of the user's hand to unlock the phone in a secure manner [52-55]. Because of its built-in motion sensors, ShakeIn is able to accurately record the distinctive and dependable biometric aspects of its users' shaking [56]. This makes it extremely difficult for an attacker to imitate a user's actions, even if the attacker witnesses the user shaking his or her phone. Furthermore, ShakeIn permits maximal operation freedom by allowing customers to tailor how they shake the phone. We deploy ShakeIn and run extensive trace-driven simulations alongside real-world tests on 20 participants and approximately 530; 555 samples of shaking data gathered over the course of many months [57-61]. In spite of being subjected to shoulder-surfing attacks, the results reveal that ShakeIn is able to obtain an error rate of only 2% on average for a limited number of shakes utilising just 35 training samples [62].
To prevent authentication-system-compromising shoulder-surfing attacks, a hybrid keyboard approach has been created. This is a password-based security system for touchscreen gadgets. As long as the user is in close proximity to the device, they will only see a single keypad on which to input their PIN. At a greater distance, though, the attacker only sees the opposite keypad [63-65]. Every time authentication is attempted, the user's keypad is randomly rearranged to prevent an attacker from learning the pattern of keys that were pushed. To assess the safety of illusion PIN, we created an algorithm based on how humans take in visual information. We made an estimate of the smallest distance an observer could be and yet understand the user's keypad input. Our research suggests that it is extremely difficult for a surveillance camera to intercept a PIN entered on a hybrid keypad while using a smartphone. A banking application makes use of this strategy. If a PIN is entered when logging into the app, the hybrid keypad will be activated [66-71].

Software Description

Python is a powerful high-level language that can be used for a wide variety of projects thanks to its interpretive nature. Python was created by Guido van Rossum and released for the first time in 1991 with a design philosophy that prioritised making code easy to read. It supplies the building blocks for readable code, whether on a micro or macro scale [72]. Van Rossum announced his retirement as leader of the language community in July of 2018. Python's dynamic type system and built-in memory management are two of its most notable features. Object-oriented, imperative, functional, and procedural programming are all supported, and the language comes with a sizable and well-rounded set of built-in tools. Many different OSes have Python interpreters. Nearly all of Python's other implementations follow the same open-source, community-based development paradigm as CPython, the reference implementation. Python and CPython are managed by the non-profit Python Software Foundation. Python's designers opted to make the language extremely extensible rather than include all of its features into its core [73-79]. This small-footprint flexibility has made integrating programmable interfaces into preexisting software a hot trend. Frustration with ABC's insistence on a large core language with a tiny standard library and difficult to extend interpreter inspired Van Rossum to envision a compact core language with a huge standard library and easy to extend interpreter [80]. Python is a programming language that allows for multiple approaches to writing code but is known for its minimalistic grammar and rejection of verbose syntax, such as that of Perl.

To call anything "smart" is not a compliment in the Python community, as Alex Martelli put it. Python's attitude is that "there should be one—and preferably only one—obvious way to do it," as opposed to Perl's "there is more than one way to do it." As a result, modifications to non-critical areas of CPython that would give modest benefits in speed at the expense of clarity are routinely rejected by the Python community. Time-sensitive functions can be moved to extension modules written in languages like C or a just-in-time compiler like PyPy can be used by a Python writer. Alternatively, you can use CPython, which compiles Python code into C and then uses that code to make API calls to the Python interpreter [81-85]. The Python team has made user enjoyment a priority in their work. This is reflected in the name of the language, which is an homage to the British comedy group Monty Python, and in the occasionally lighthearted tone of tutorials and reference materials, such as the use of spam and eggs (from a famous Monty Python sketch) as examples rather than the more conventional for and bar [86].

The term "pythonic" has multiple interpretations in the Python community, all of which have to do with the language's programming style. Pythonic code leverages Python idioms effectively, reads like it was written by someone who is fluent in the language, and adheres to Python's emphasis on simplicity and clarity. On the other hand, "unpythonic" code is described as being particularly difficult to understand or as reading like a clumsy transcription from another programming language [87-95]. Pythonists, Pythonistas, and Pythoneers are common names for Python's users and fans, especially those who are considered competent or experienced. Python is a high-level, object-oriented programming language that is interpreted and has dynamic semantics. In addition to its utility as a scripting or glue language for
connecting preexisting components, the language's high-level built-in data structures, dynamic typing, and dynamic binding all contribute to its appeal for Rapid Application Development. Readability is emphasised and maintenance expenses are decreased because to Python's straightforward syntax. Program modularity and code reuse are fostered by Python's module and package support. The Python programming language and its comprehensive standard library are open-source and freely distributable in source or binary form for all major platforms. Python's greater productivity is a major draw for programmers. Since compilation is not required, the iteration between editing, testing, and debugging is lightning quick. Because Python never generates a segmentation fault in response to an error or invalid input, debugging is a breeze. In its place, the interpreter throws an exception if it encounters a problem. When an exception is not handled by the programme, the interpreter displays a stack trace [96-101]. A debugger that works on the source code level allows you to view the values of local and global variables, evaluate expressions, place breakpoints, walk through the code line by line, and so on. The debugger is a testament to Python's ability to look inward. However, adding a few print statements to the source is typically the easiest method to debug a programme; the fast edit-test-debug cycle makes this simple approach quite effective. In the 1980s, when Python was first being developed, it was led by Guido van Rossum. The Python Software Foundation now maintains and updates the language. Python's flexibility as a multiparadigm language means that developers are free to choose from a variety of approaches, including object-oriented, imperative, functional, and reflective, when implementing their code. Python has many applications beyond only the web, including numerical programming, game development, and access to serial ports [102-109].

Python's rapid growth is due to two features that set it apart from other languages:

- Python is an interpreted language, which means that compilation is performed automatically before a programme is executed. Python, being a high-level language, hides the complexity of its code behind a layer of abstraction. Python's emphasis on this abstraction makes it accessible to even inexperienced programmers.

- Python code is typically shorter than competing languages' equivalents. Python's quick development periods come at the expense of a minor delay in execution. Python programmes run more slowly than those written in fully compiling languages like C or C++. With modern computers' processing speeds, however, speed differences are typically only seen in benchmarking tests and not in actual use. Python is typically preinstalled on Linux and Mac OS X computers [110].

BACK END: MY SQL

In 2008, MySQL had the most users of any open-source RDBMS; it is a server that allows multiple users to access the same set of databases at once. MySQL's developers have released the software's source code under a number of different licences and proprietary agreements, including the GNU General Public License. One for-profit company, the Swedish corporation MySQL AB (which is now owned by Oracle Corporation), was responsible for developing and promoting MySQL.

MySQL is a frequently used database for web applications and a key part of the LAMP (Linux, Apache, MySQL, Perl/PHP/Python) open-source web application software stack. MySQL is a popular choice for free/open source software projects that need a powerful database management system. Several premium editions with additional features are available for commercial use [111-114]. MySQL databases are used by a wide variety of LAMP-based applications, such as TYPO3, Joomla, Word Press, phpBB, MyBB, and Drupal. Wikipedia, Google (though not for searches), Imagebook, Twitter, Flickr, Nokia.com, and YouTube are just some of the many well-known, massive-scale Web products that employ MySQL [115-119].

MySQL is primarily an RDBMS; there are no graphical user interface (GUI) tools for managing MySQL databases or the data contained therein. MySQL "front-ends," desktop software and web apps, and the command line tools it comes with are all that users need to create and manage MySQL databases,
construct database structures, back up data, inspect status, and operate with data records. MySQL Workbench is Oracle's official collection of front-end tools for MySQL, and it's available for free [120].

**Graphical:**
MySQL AB's official MySQL Workbench is a no-cost integrated environment that provides graphical tools for managing databases and creating new ones [121-124]. The former software suite, MySQL GUI Tools, has been replaced by MySQL Workbench. MySQL Workbench is a front-end for MySQL that, like other third-party products, allows users to manage database design and modelling, SQL development (in place of MySQL Query Browser), and Database management (replacing MySQL Administrator) [125]. There are two versions of MySQL Workbench: the free and open-source Community Edition, which can be downloaded from the MySQL website, and the paid, premium Standard Edition, which adds to and improves the functionality of the former [126].

**System Design**
The structure, behaviour, and perspectives of a system are conceptualised in a model called the system's architecture [127]. A formal description and representation of a system arranged to facilitate reasoning about the system's structures and behaviours is known as an architecture description. A system's architecture can include the parts that make up the system, their outwardly apparent characteristics, and the connections (e.g., the behaviour) between them. It can serve as a blueprint for acquiring the necessary components and creating the necessary infrastructure to put the system into action [128-129]. Efforts have been made to formalise a set of languages for describing the architecture of a system; these are known as architectural description languages (ADLs) (fig.2).

![Diagram](image)

**Figure 1: System Architecture**

**Use Case Diagram**
A Use Case Is A Set Of Instructions On How A Certain Role (Called A "Actor" In Unified Modeling Language) And A System Collaborate To Accomplish A Specific Task. The Player Can Be A Living Being, A Machine, Or The Passage Of Time. Use Cases Are Taken To A Higher Degree In Systems Engineering Than They Are In Software Engineering, Typically Symbolising Missions Or Stakeholder Goals.

The Class Diagram Does Not Change. It Stands In For The Unchanging Perspective Of A Programme. To Generate The Executable Code Of A Software Programme, The Class Diagram Is Used To Visualise, Describe, And Record Various Parts Of The System. The Class Diagram Defines The Parameters Of A
Class And The Methods It Can Perform. Since No Other UML Diagram Can Be Directly Translated With Object-Oriented Languages, Class Diagrams See Extensive Use In The Modelling Of Such Systems.


**Entity Relationship Diagram**


This Section Of The Tutorial Deals With The User's Credentials. In Order To Utilise The Banking Software, The User Must First Register For An Account. A User's First Name, Last Name, Address, Account Information, Pin, User Name, And Password Are All Examples Of Mandatory Fields During Registration. The Pin Is Expected To Be A Four-Digit Sequence Of Numbers. You Can Use Any Regular Keypad To Check Your Login And Password. A Digital Keypad Will Be Used To Input The Pin.


Admin Needs To Register For An Account In Order To Use The Atm Software. Admin Id, Admin Name, And Password Are Required For Signup. The Database Will Hold These Specifics. Using Their Verified Credentials, Admin Can Enter The System. While Entering Their Pin, Customers Can Use Other Atm Features. The Administrator Can See Who Each User Is And What Each User Has Purchased.


**System Testing**

It is possible to prepare and execute tests in a methodical fashion. The computerised system is tested in stages, starting with individual modules and ending with their integration. Testing is essential to the health of any system, so it's essential that it be done before anything else. Following the aforementioned
goals during testing will help find bugs in the programme. Testing also shows that the software appears to execute as expected and that performance goals have been met. A programme can be tested in three distinct ways. Implementation efficiency tests look for ways to reduce the size and runtime of a correct programme. It's an examination of the algorithm's implementation that takes place during the code-refinement process. Computational complexity tests are essentially an experimental investigation of an algorithm's complexity or a comparison of two or more algorithms that achieve the same goal (fig.2).

There are other guidelines that can be used as benchmarks: 1. The goal of testing is to detect bugs in a programme by running it. Following the aforementioned goals during testing will help find bugs in the programme. Testing also shows that the software appears to execute as expected and that performance goals have been met. A programme can be tested in three distinct ways. Correctness tests are meant to ensure that a software functions as intended. It's not as simple as it seems, especially with larger projects. Implementation efficiency tests look for ways to reduce the size and runtime of a correct programme. It's an examination of the algorithm's implementation that takes place during the code-refinement process. Experimental investigation of the difficulty of an algorithm, or comparison of two or more algorithms that solve the same issue, includes tests for computational complexity.

Conclusion

The suggested system describes how a hybrid keypad is used in an automated teller machine. Creating a PIN-based authentication mechanism that is secure against shoulder surfing assaults was the primary focus of our study. We developed Illusion PIN for this purpose. The proposed system has introduced the concept of safety distance to quantify the resistance level against shoulder-surfing. The visibility algorithm required us to model the fundamentals of the human visual system. Several simplifying assumptions were made during this process, which reduces the precision of our results. This means that the visibility index is lower for a hybrid keypad, even though the numbers appear to be as legible to the user as they would be on a digital keypad. Seeing a digit that is even faintly visible is considered a severe distortion, therefore this makes sense when the reference buttons are all the same colour. This project will continue with the development of a proposal for an Android-based banking application and the implementation of extremely secure measurements based on Digital PIN authentication or Bright Pass authentication.

Reference


of the Side Channel Attacks for Enhancing the Network Security”, Pre-print, 2022.

84. Naveen S Pagad, N Pradeep, Tulika Chakrabarti, Prasun Chakrabarti, Ahmed A Elngar, Martin Margala, Mohammad Nami, Neha Sharma, Samuel Frimpong, “Clinical XLNet-based End-to-End Knowledge Discovery on Clinical Text Data using Natural Language Processing”, Pre-print, 2022


