ISSN-P: 2807-5987

Enhanced Signature-based Mechanism using User Verification Policy

آلية محسنة قائمة على التوقيع باستخدام سياسة التحقق من المستخدم

ISSN-E: 26632806

ISSN-P: 2807-5987

1. Introduction

The idea of creating a manual signature system based on the employee id number and signature font to verify that the user is still the same and works within his permission to reduce the loss of follow-up of many accounts within the organization that may have permissions that may affect the organization's work or perhaps trading accounts between organization employees or using them after the employee's period of employment, the idea is to schedule validation of u. The idea of creating a manual signature system based on the employee id number and signature font to verify that the user is still the same and works within his permission to reduce the loss of follow-up of many accounts within the organization that may have permissions that may affect the organization's work or perhaps trading accounts between organization employees or using them after the employee's period of employment, the idea is to schedule validation of its unique qualities, such as hand geometry, iris scan, and fingerprints, biometrics for user identification is on the increase. One of the most practical approaches for identifying and verifying human beings has been signatures. A signature may be termed a behavioral biometric, as it changes depending on many elements such as mood, fatigue. The challenging aspects of automated signature identification and verification have been a true motivation for researchers for a long time. Signature verification research has been active for some years (K. Han, 1996)and is still being investigated. Online verification must be differentiated from offline verification, as the number of features, which may be extracted from online mediums, exceeds those obtained from offline verification time; pressure and speed can be extracted from online modes of verification. The GSC (Gradient, Structural, and Concavity) feature extractor provided results as high as 78% for verification and 93% for identification. Various classifiers, like Support Vector Machines (SVMs) and Hidden Markov Models (HMMs) (S. Chen, 2005), have also been successful in offline signature verification; SVMs provide an overall better result than the HMM-based approach. Research into person identification/verification, including physical traits, fingerprint, and signature analysis, has also been investigated. Choosing a robust set of features is crucial for both the application and the classifier in pattern recognition (A. Kholmatov, 2005). To conduct signature verification, using the direction distribution, moment feature, stroke width distribution, and grey distribution. Previous work using the Modified Direction Feature generated encouraging results, reaching an accuracy of 81.58% for cursive handwritten character recognition. As an extension to previous work, the research in this paper adapts, extends, and investigates MDF with signature images. Specifically, several features have been combined with MDF to capture various structural and geometric properties of the investigated signatures. The verification process implies the usage of forged signatures, discriminating the genuine from the developed (Stéphane Armand, 2006).

2. Related Work

As in (Gaopeng Xie, 2021), The cloud storage rising popularity and the quick expansion of data have also become a classic topic, as has to guarantee the integrity of the data on the cloud. This study proposed an efficient cloud data integrity verification scheme based on blockchain. In the system, the blockchain network is used to solve some limitations of the traditional centralized audit and improve the efficiency and security of the scheme. And it based on the assumption of the SIS problem, the system may resist the threat of quantum computing, and by combining lattice signature and cuckoo filter, it simplifies the verification process user, solving part of the problem of the insufficient computing power of users. The proposed scheme's performance is evaluated, and the result shows that the system is provably efficient. A closer combination of blockchain and integrity verification schemes needs to be explored in future work, and more comprehensive system characteristics need to be satisfied.

In (Dalish, 2021), the idea is to build a manual signature system based on employee id number with the signature font to verify that the user is still the same and works within his permission to reduce the loss of follow-up of many accounts within the organization that may have permissions that may affect the work of the organization or perhaps trading accounts between the organization employees or use them after the end of the employee's period of work, the idea is to schedule validation of users by an intelligent signature. The signature recognition system is modern, and it needs a lot of research to develop. The study does not focus on the image recognition mechanism and algorithms. Still, it tries to create an automatic recognition system for the manual signature for its accuracy and the difficulty of plagiarism and forgery to renew the account work in the facility to reduce the burden on users to follow up and restore their powers. The origin of any account created is closed after a specified time by the IT department and the system administrator.

According to ETSI study of (Signature, 2008), a signature policy is a set of criteria for developing electronic signature validation, under which electronic signatures can be considered valid. It contains rules defining the signature attributes that the signatory must provide and regulations on the use of Trusted Third Parties. A signature policy includes the following elements, is the identification of one or more "trusted points" and the rules allowing to build a certification path between the signatory's certificate and one of these trusted points, which Means obtaining a time reference intended to position in time the signature of the signatory (by time stamping), Means to verify the revocation status of each certificate of the certification path with this time reference, The attributes which the signatory's certificate must contain (OID of the certification policy, key usage), Types of features which, in addition to the reference of the signatory's certificate, must be signed jointly with the document (reference to a signature policy, type of engagement, supposed date of signature, format of the paper, supposed role of the signatory, supposed place of signature).

The research of (TS, 2012), provides an algorithm for validating electronic signatures, focusing on signature validation of "ancient" electronic signatures, in which certificates may have expired, been revoked, or the algorithm's usage term has expired. It accomplishes this by emphasizing the signer's or preceding verifiers' security measures and guaranteeing that such signatures can still be validated. It is agnostic to the kind of security measures. At the same time, it primarily aims at Advanced Electronic Signatures, which provide such features intrinsically; It also allows for variants, such as traditional archiving services with non-cryptographic security mechanisms. The presentation of the algorithm tries for clarity and understandability. It is not assumed or recommended that the algorithm be implemented as described. Efficiency and the other implementation aspects were not considered. However, a conformant implementation will provide the same results as the algorithm here would. An efficient performance will need to reorder algorithms, use caching of results wherever possible, and do things in parallel. A signature validation policy drives signature validation. Such policies are supported by the algorithm provided here. The validator, represented by the driving program, is supposed to supply such a policy in various ways, such as a formal policy, a set of configuration parameters, or through the way the algorithm has been built. The term constraint refers to a single policy rule that governs the algorithm's decisions to minimize confusion. As mentioned, a formal signature policy can give a set of restrictions that can be utilized alone or in combination with additional constraints (coming from local configuration).

3. Problem Statement

The verification mechanism is based on matching the shape and direction of movement as it is difficult to compare with a single possible signature for this, we need possible copy’s for each user; many algorithms specialized in this regard need to be developed further to increase efficiency, need physical equipment to read hand signature like smart board or PC application in the (account activation center) location or add for each PC.

Signature verification can Limit the use of unauthorized accounts with it permissions that can be exploited between employee accounts, by temporarily closing the account to be reactivate according the time specified by the Users Manager.

4. Project Goals and Objectives

- Apply the importance of the signature verification system to differentiate the genuine from the forgeries.
- warning Using the random forgery that the signature sample belonged to a writer, which was different to those used in the signature model.
- The study provides a protection profile that allows presenting all the common security objectives for sponsors of electronic signatures applications.

- The objective of this study is to validate the signer's signature in many ways.
- The objective for the study is to ensure the authenticity of the signature policy and subsequently assess whether to accept or reject the transaction.

5. Methodology

- Developing a Biometric signature authentication system can also be replaced with fingerprint devices, which can now be bypassed and facial recognition. It can also be avoided, but it may require additional skill and tools, while the scheduled manual signature system by entering with id to improve comparing process.
- The effective methods to perform off-line signature verification using unique structural features extracted from the signature's contour.
- In identifying a signature or performance of verification, many steps should be performed. After preprocessing all the signatures from the database by converting them to a portable bitmap format, their boundaries are extracted to facilitate the extraction of features.
- Experiments are performed with the “Grupo de Procesado Digital de Senales” (GPDS) signature database.
- Extract the boundary of each signature before the feature extraction process. As it uses neural classifiers, the amount of data used as input to perform verification is an important parameter, having a large input vector size could dramatically increase the complexity and training time of the classifier and potentially decrease the accuracy of the system.

6. Work details and time constraint

- Study the concept of Verification Policy and its main models.

- Propose a systematic literature review for applying Verification Policy mechanisms.

- study the enhanced mechanisms by using User Verification Policy.

- Propose a novel security framework to develop the verification policies.

6.1 Time line

The project timeline represents the sequence of activities or a strategy that is viewed sequentially. The approach we select for our research roadmap depends on numerous aspects, like our workplace and the theories that we chose to describe.

6.1.1 GANTT CHART

We preferred the concept of having a map of overlapping lines defined as the Gantt chart, displaying the work activities we assigned ourselves as well as the performance of activities side

ISSN-P: 2807-5987

by side. Below is a Gantt chart demonstrating the advancement of our assigned tasks alongside time.

	First month			Second month			Third month		
Background reading									
Proposal\initial meetings									
Literature review									
Research methods planning									
Data collection									
Check on progress\ date analysis									
Submit some draft work									
Discuss conclusion									
Final meeting									
Final draft									

7. Anticipated outcomes

After establishing a thorough study about Enhancing Signature-based Mechanism using User Verification Policy. We anticipate to provide a better solution for boosting data privacy and security in many fields.

ISSN-E: 26632806

8- References

- A. Kholmatov, a. B. (2005). Identity Authentication using improved online signature verification method.
- Dalish, M. (2021). User verification policy by signature. Aljouf : Aljouf university.
- Gaopeng Xie, Y. L. (2021). Blockchain-Based Cloud Data Integrity Verification Scheme with. College of Computer Science and Electronic Engineering, Hunan University.
- K. Han, a. I. (1996). Handwritten Signature Retrieval and Identification", Pattern Recognition.
- S. Chen, a. S. (2005). use of Exterior Contour and Shape Features in Off-line Signature Verification.
- Signature, P. (2008). Protection Profile Electronic Signature Verification Module.
- Stéphane Armand, M. B. (2006). Off-line Signature Verification using the Enhanced Modified Direction Feature.
- TS, E. (2012). Electronic Signatures and Infrastructures (ESI);Signature validation procedures and policies.

ISSN-P: 2807-5987

ISSN-E: 26632806