WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Internet Banking Using Fingerprint and Iris Authentication

Jaya Suriya S[1], Mr. P. Anbumani[2]

PG Student[1], [2]M.C.A., M.Phil, Net., Associate Professor

Krishnasamy College of Engineering and Technology, Cuddalore.

ABSTRACT

Internet banking is a product of ecommerce in the field of banking and financial services. Inwhat can be described as business to customer domain for banking industry, Internet bankingoffers different online services like balance enquiry, fund transfer, opening account etc. Mostly, these are traditional services offered through internet as a newdelivery channel.Banks are also offering payment services on the behalf of their customers whoshop in different e-shops, emalls etc. While the internet offers enormous advantages and opportunities, it also presents various security risks. In order to secure online transactions, so we propose "Secure Internet banking System" which uses Biometric features to ensure customer activities in a secure way.

INTRODUCTION

A web service is a method of communication between two electronic devices over the World Wide Web. A web service is a software function provided at a network address over the web or the cloud, it is a service that is "always on" as in the concept of utility computing. The W3C defines a "Web service" as software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. Interoperability - This is the most important benefit of Web Services. Web Services typically work outside of private networks, offering developers a nonproprietary route to their solutions. Services developed are likely, therefore, to have a longer life-span, offering better return on investment of the developed service. Web Services also let developers use their preferred programming languages. In addition, thanks to the use of standards-based communications methods, Web Services are virtually platform-independent. Usability - Web Services allow the business logic of many different systems to be exposed over the Web. This gives your applications the freedom to chose the Web Services that they need. Instead of re-inventing the wheel for each client, you need only include additional application-specific business logic on the clientside. This allows you to develop services and/or client-side code using the languages and tools that you want.Reusability - Web Services provide not a component-based model of application development, but the closest thing possible to zero-coding deployment of such services. This makes requirements of very large data sets as examples it easy to reuse Web Service components as appropriate and we hope that it would act as a catalyst for the

LITERATURE SURVEY

Metered in gigabyte/month. For an increased I-A survey of cloud storage facilities level of scalability, availability, and durability,

AUTHORS: H. Dewan and R. C. Hansdah some customers may want their data to be There are many applications such as software for replicated on multiple servers across multiple processing customer records in telecom, patient records data centers. The more copies the CSP is asked to in hospitals, email processing software accessing a store, the more fees the customers are charged. single email in a mailbox etc. which require to access a Therefore, customers need to have a strong single record in a database consisting of millions of guarantee that the CSP is storing all data copies records. A basic feature of these applications is that that are agreed upon in the service contract, and they need to access data sets which are very large but all these copies are consistent with the most simple. Cloud computing provides computing recent modifications issued by the customers. In requirements for these kinds of new generation of this paper, we propose a map-based provable applications involving very large data sets which multicopy dynamic data possession cannot possibly be handled efficiently using traditional (MBPMDDP) scheme that has the following computing infrastructure. In this paper, we describe features: 1) it provides an evidence to the storage services provided by three wellknown cloud customers that the CSP is not cheating by storing service providers and give a comparison of their fewer copies; 2) it supports outsourcing of features with a view to characterize storage dynamic data, i.e., it supports block-level operations, such as block modification, insertion,

SYSTEM ARCHITECTURE:

privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of

security solutions for a trustworthy public cloud environment.III-Provable multicopy dynamic data possession in cloud computing systems

AUTHORS: A. F. Barsoum and M. A. Hasan Increasingly more and more organizations are opting for outsourcing data to remote cloud service providers (CSPs). Customers can rent the CSPs storage infrastructure to store and retrieve

PROPOSED SYSTEM

deletion, and append; and 3) it allows authorized users The proposed biometric authentication system to seamlessly access the file copies stored by the CSP. using eye tracking and fingerprint authentication We give a comparative analysis of the proposed aims to provide a more secure and reliable MBPMDDP scheme with a reference model obtained authentication method than the existing systems. by extending existing provable possession of dynamic The system architecture is based on a clientserver single-copy schemes. The theoretical analysis is model, where the client is responsible for validated through experimental results on a capturing the biometric data and sending it to the commercial cloud platform. In addition, we show the server for processing and decisionmaking. The security against colluding servers, and discuss how to proposed system doesn't uses any hardware or identify corrupted copies by slightly modifying the devices to scan the fingerprint

EXISTING SYSTEM

Comparison with the registered fingerprint in thedatabase. The decision-making of the proposed

- The existing authentication systems rely system analyzes the biometric data from the eye primarily on the use of passwords or PINs, which are tracking and fingerprint authentication modules vulnerable to security breaches and attacks such as using string matching to determine whether to password guessing, phishing, and social engineering. grant access or not. The system also includes a Other authentication methods such as tokens and smart database to store the biometric data and user cards are also available, but they can be costly and information securely. Overall, the proposed inconvenient for users to carry and use. system provides a practical solution to the problem of secure authentication and can be
- Biometric authentication has emerged as a further improved and extended in future research. more secure and reliable alternative to traditional The system is expected to achieve high accuracy authenticatio methods. Existing biometric and reliability and provide a more secure and authentication systems use various biometric convenient authentication method for users.modalities such as fingerprint, face recognition, voice

MODULE DESCRIPTION

recognition, and iris recognition to authenticate users.However, these systems can still be vulnerable to 1.Eye Tracking spoofing attacks where an attacker can fool the system Template-Matching Template-Matching is a by presenting fake biometric data or images. well-known method for object detection. In our template matching method, a standard eye pattern

- Eye tracking technology has been used in is created manually and given an input image, the various applications such as market research, usability correlation values with the standard patterns are testing, and gaze-based interaction, but its potential for computed for the eyes. The existence of an eye is biometric authentication has not been fully explored. determined based on the correlation values. This The combination of eye tracking and fingerprint approach Has the advantage of being simple to authentication provides a more robust and secure implement. However, it may sometimes be authentication method that can resist spoofing attacks Inadequate for eye detection since it cannot and improve the overall security of the system. effectively deal with variation in scale, pose and shape. Face detection : Performs scale invariant face detection Eye detection : Both eyes are detected as advantage of being simple to implement. a result of this step Eye feature extraction : Features of However, it may sometimes be inadequate for eyes are extracted at the end of this step Face Detection finger detection since it cannot effectively deal

Future Enhancements:

Multifactor Authentication: Consider implementing a multi-factor authentication approach that combines biometric authentication with additional security measures such as one-time passwords (OTP), SMS verification, or hardware tokens. This adds an extra layer of security and makes it even more challenging for attackers to breach the system.

Continuous Authentication: Explore the possibility of implementing continuous authentication, where the user's biometric data is continuously monitored throughout their banking session. This ensures that the user remains authenticated even during their online banking activities, reducing the risk of unauthorized access if the user steps away from their device momentarily.

Behavioral Biometrics: Investigate the use of behavioral biometrics, such as typing patterns, mouse movements, or touchscreen gestures, to further enhance security. Analyzing these unique behavioral patterns can help detect anomalies and flag suspicious activities, providing an additional layer of protection against fraud.

Advanced Encryption: Continuously update and strengthen the encryption protocols used to protect sensitive customer data. Keep up with the latest encryption standards and algorithms to ensure data privacy and prevent unauthorized access to user information.

Secure Communication Channels: Implement secure communication channels, such as Transport Layer Security (TLS), to encrypt data transmission between the user's device and the banking servers. This prevents eavesdropping and protects sensitive information from interception.

Robust Fraud Detection: Invest in advanced fraud detection systems that utilize machine learning algorithms and artificial intelligence to identify and prevent fraudulent activities. These systems can analyze patterns, detect anomalies, and proactively flag suspicious transactions, providing early warning signs of potential fraud.

User Education and Awareness: Focus on educating users about the importance of strong security practices, such as not sharing biometric data, using secure devices, and regularly updating their banking application. Provide clear guidelines and resources to help users understand and utilize the biometric authentication features effectively.

Conclusion:

Implementing secure internet banking using fingerprint and iris authentication can greatly enhance the security and convenience of online banking services. These biometric authentication methods provide a robust and reliable way to verify the identity of users, mitigating the risks associated with traditional username/password-based authentication. By utilizing fingerprints and iris scans, banks can significantly reduce the chances of unauthorized access and protect sensitive customer information.