PERSPECTIVE

Safe as a Bank: Iris Scan Biometrics for Secure Data Access

Secure confidential data for banks with a cutting-edge safety net

– Mohan Kumar, Rakhi Agrawal, Dhruv Chauhan

Infosys®

Importance of Document Security in Banking

The banking industry conducts business via electronic documentation. Banks manage customer information, financial data, and products through electronic documents. The sensitive nature of information demands the highest level of security to prevent unauthorized access.

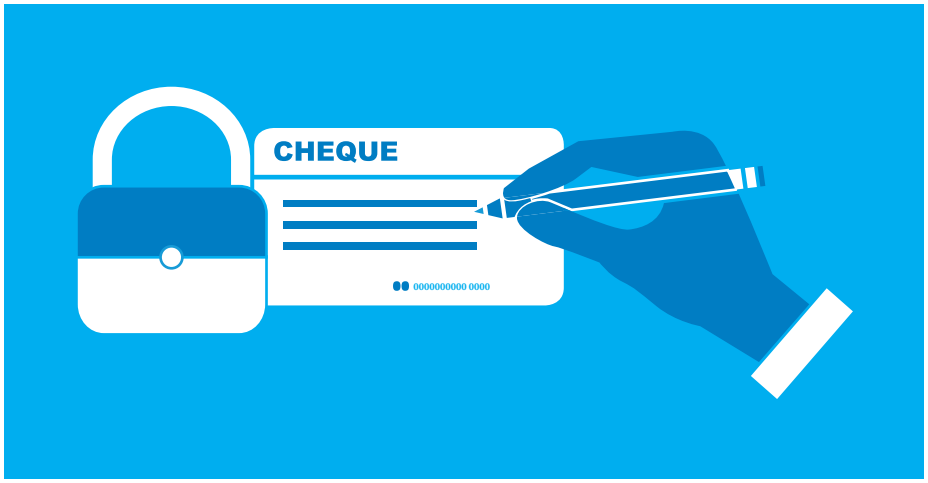
A security breach at a bank can result in a severe loss of business and reputation. A biometric security system ensures secure and authorized access to critical data residing in electronic documents. Our point of view discusses how biometric security protects business interests and safeguards the privacy of stakeholders in banking. We offer a nuanced perspective:

- The business imperative of confidential data
- Limitations of current methods to protect electronic documents
- Minimizing security breaches by adopting biometric security
- Biometric security clearance for top secret information

Banking Imperative: Confidentiality of Data

The widespread use of electronic documents makes the security of top secret documents critical for banking. Confidential financial and customer data require stringent user and security protocols. When unauthorized persons gain access to sensitive data, it can dilute the brand, result in loss of business, and erode the confidence of customers. Banks can uphold data security by adopting a robust policy to prevent breach of security and unauthorized access.

Financial institutions must address the data imperative: protect and prevent. Data must

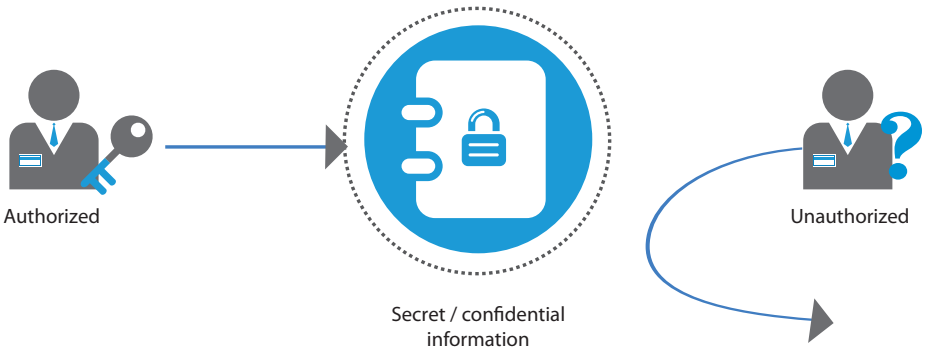


be secured to protect it from unauthorized access and prevent any material or collateral damage. It requires information to be classified under several categories based on the damage caused by a security breach.

Business Confidential

Confidential information constitutes documents, pictures, audio, and video material underlined by a privacy statement. The information can be owned by an individual or a company. The right to access or share such private information must be granted to persons on the condition that violations and breaches will be avoided.

Confidential information should be accessed only by authorized persons and through authorized channels. It is advisable that owners issue a signed authorization letter to users for safeguarding data. If a person is unauthorized or the channel is not authenticated, it results in unauthorized access as illustrated below:



In a company, customer data is confidential and can be accessed only by authorized persons. Similarly, details of employees can be viewed only by the HR department or other authorized personnel.

Governments have highly secret intelligence, defense and financial data. It can be accessed only by a select few authorized persons.

Hospitals have patient records. Such confidential data should not be accessible to persons outside the hospital.

R&D data is top secret. Any leakage can cause a significant loss to the company.

Companies must safeguard their business interests by securing sensitive customer information, financial records and product data. Top secret information demands a high level of security to prevent breaches that could cause serious damage.

There are several security protocols to safeguard confidential documents from unauthorized access such as passwords and encryption. However, these protocols do not guarantee secure and authorized access. Information can be leaked if it is unprotected, accidentally stored at a place with unauthorized access, or shared by authorized persons.

Security Clearance

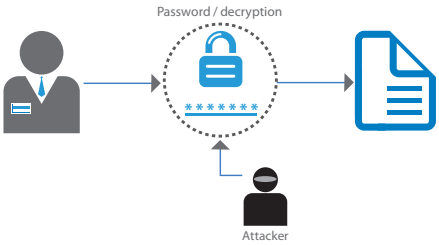
Security clearance is granted to individuals for secure access to information classified under different levels of confidentiality. Governments and companies have a formal process to allow access of sensitive information to employees. Apart from security clearance, companies determine whether an individual needs to know the information. Access to classified information must be strictly on a 'need to know' basis and not based on rank, position or security clearance.

Traditional Security Methods and Challenges

The traditional methods of access control include knowledge-based identification systems for document security. The security systems adopted include:

1. Passwords / PINs: The owner sets a unique personal identification number (PIN) or password (combination of letters, numbers and special characters) to access the document with secure information.
2. Encryption / decryption: When information is transmitted across the network, it is encrypted before the transfer to protect information from a security breach. The receiver can decrypt the secure information before gaining access. It involves a secret key, which is shared between the sender and receiver.

A smart combination of letters, numbers and special characters in a password may not be easy to guess for hackers, but it is difficult for users to remember. If the user has access to multiple documents, it is difficult to remember multiple passwords / PINs or retain one master password. Keystroke recording software can be installed on personal computers to capture keystrokes and trace passwords.



Moreover, a virtual keyboard is not safe in a public computer since clicking virtual keys is comparatively slower than typing a password. Most importantly, traditional methods are unreliable as they do not recognize users as unique individuals.

In a traditional security system, the user establishes credentials based on PINs, passwords, decryption keys, or tokens. However, it does not prove that the user is the real owner.

The risks of traditional security systems outweigh the positives:

Advantages

1. No devices are required
2. Cost-effective
3. Registration / recording of users' physical information is not required
4. Can be accessed anywhere, without the support of specific devices

Disadvantages

1. Users must remember passwords for every document
2. Owners must provide a unique password for each document to minimize the loss of information in the event of a security breach
3. High possibility of being leaked, shared or distributed intentionally or accidentally
4. Can be easily hacked

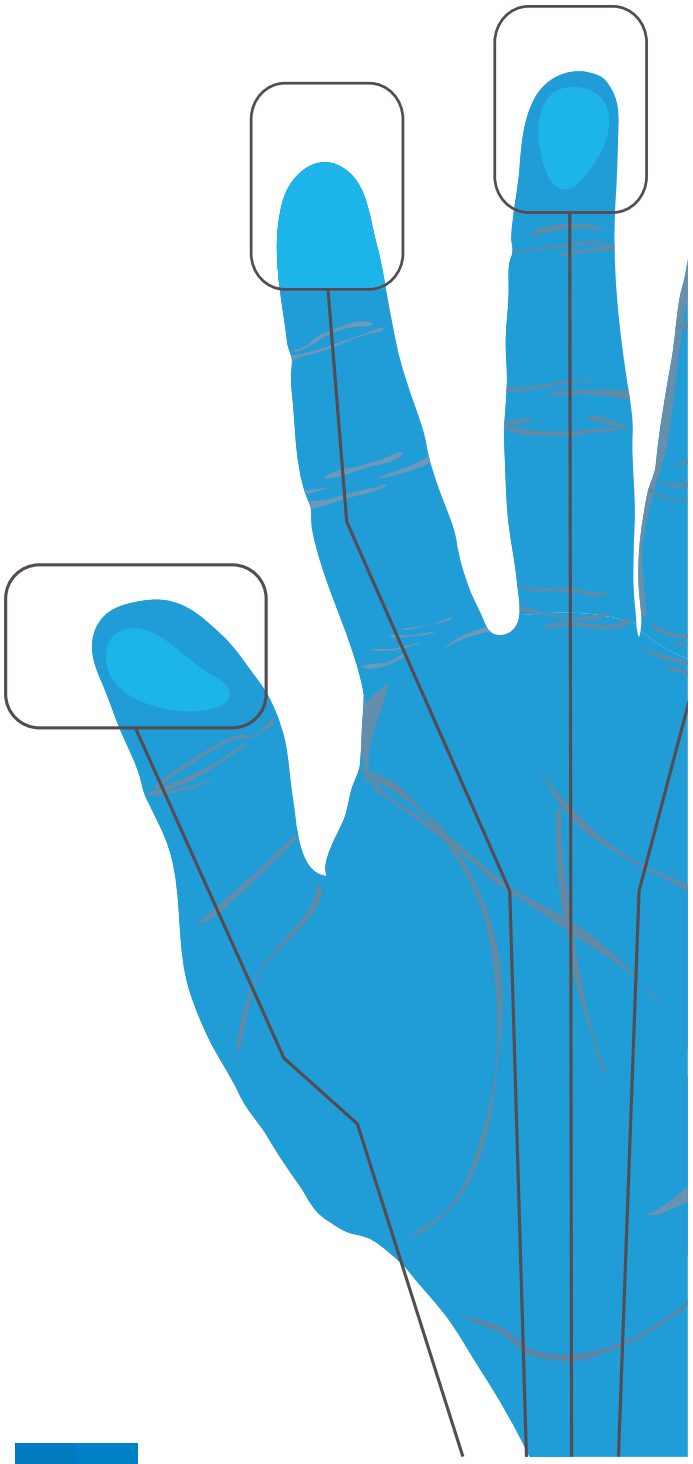
5. High risk due to proliferation of unique passwords to access sensitive documents
6. Access by authorized users is blocked when the password is lost or forgotten

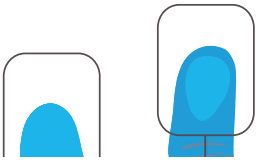
Degrees of Confidentiality

Information is confidential when it is deemed to be sensitive. Accordingly, access is restricted to a specific person or groups of people by law or regulation. A formal security scan and clearance is required to access the information. The security clearance process involves a stringent background investigation. Documents are classified under different levels of confidentiality based on the degree of sensitivity. The classification safeguards information from being used to endanger national or business interest.

Nations use a classification system to protect sensitive information and assess the impact of security breaches:

1. Top secret: Information can cause 'exceptionally grave damage' to national or organizational security. It is the highest level of classification.
2. E.g. surface-to-air guided weapons policy, reports on weapons, military plans, etc.
3. Secret: Information can cause 'serious damage' to national or organizational security.
4. E.g. allied geographical section of the army, terrain handbooks, war information, etc.
5. Confidential: Information can cause 'damage or be prejudicial' to national or organizational security.
6. E.g. confidential annexures, meetings, political plans, reports, etc.
7. Restricted: Information can cause 'undesirable effects'.
8. E.g. memorandum by defense officials, patient health information, etc.
9. Unclassified: Information not included in the above categories have no potential to cause damage and can be viewed without security clearance.
10. E.g. names, address, zip codes, phone codes, states, cities, routes, time tables, etc.





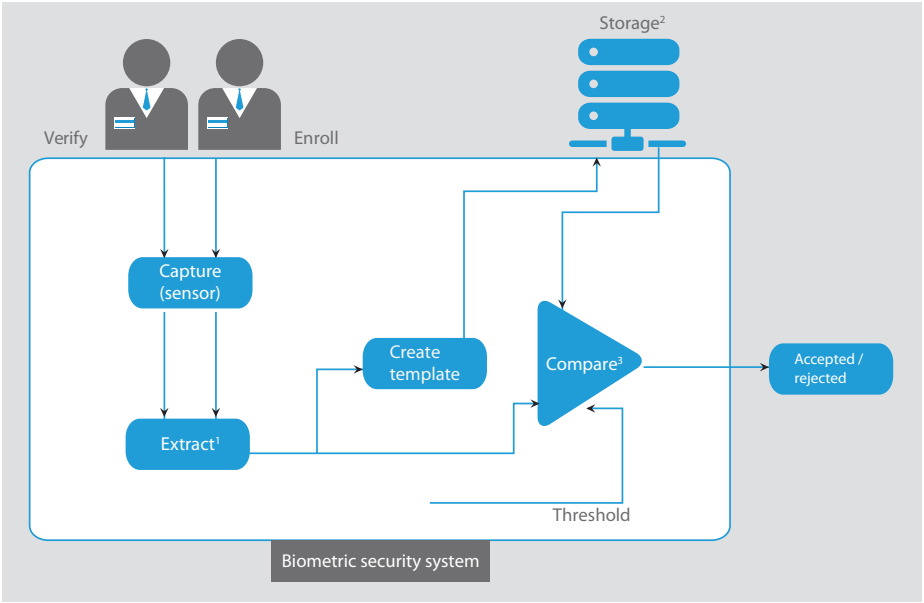
Biometrics Security

Biometrics involves the identification of human beings by their unique characteristics or traits. In computer science, it is used for access control based on the physical characteristics of a person. The biometric data is used for security clearance since it does not change during the lifetime of a person. Biometric identification technologies cover fingerprints, eyes, hands, DNA, speech, and facial characteristics.

Biometric security is a pattern recognition system that identifies the individual by establishing the authenticity of specific physical or behavioral attributes of a user. Uniqueness is the primary criterion of biometric data. The system recognizes each user as a unique individual. The system collects and stores data to verify personal identity.

A biometric security system combines biometric data systems and biometric recognition / identification technologies. Individuals can access the biometric security system by providing their unique characteristics or traits that are matched to a database. If the information is authenticated, the locking system provides access to the user. The locking and capturing system activates and records information of users who access data.

The functionality of the biometric system is illustrated below. The system recognizes an individual from a group of people based on unique personal traits.

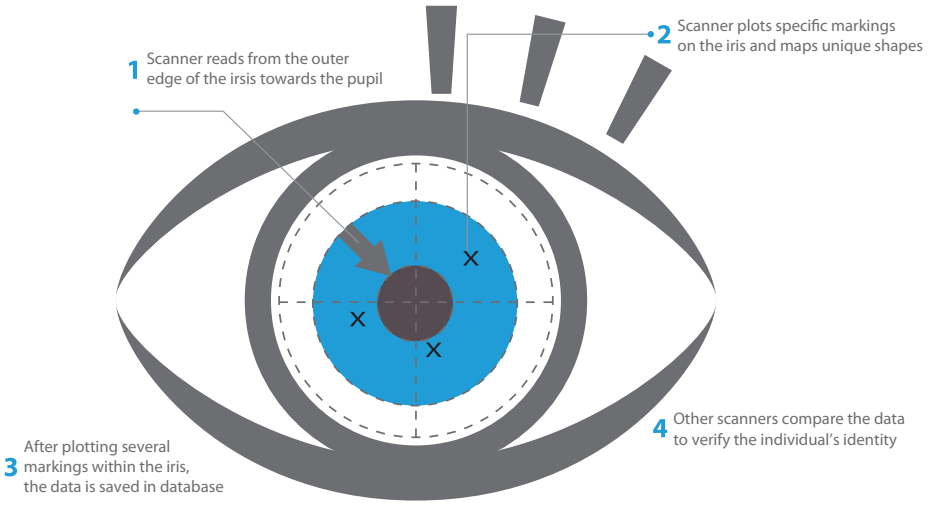


1. The extraction feature processes biometric data. The output of the module is a set of extracted features suitable for the matching algorithm. During the extraction process, the module may evaluate the quality of biometric data input.
2. Biometric templates are stored in a database. They can also be stored in user-held media such as a smartcard, in which case there must be a link between the user and biometric template (e.g. an attribute certificate).
3. The biometric matching algorithm compares current biometric features with the stored template. The predetermined security threshold level may be a parameter of the matching process. The result of matching can be an 'accept' or 'reject' message. If there is no match, a score quantifying the correlation between the template and current biometric sample is generated to enable decision making.

Iris Recognition

Iris recognition methods analyze more than 200 points of the iris, including furrows, rings, corona, freckles, and other structures. After recording data of individuals, the system saves information in a database to compare it when a user seeks access.

Iris recognition is one of the most accurate



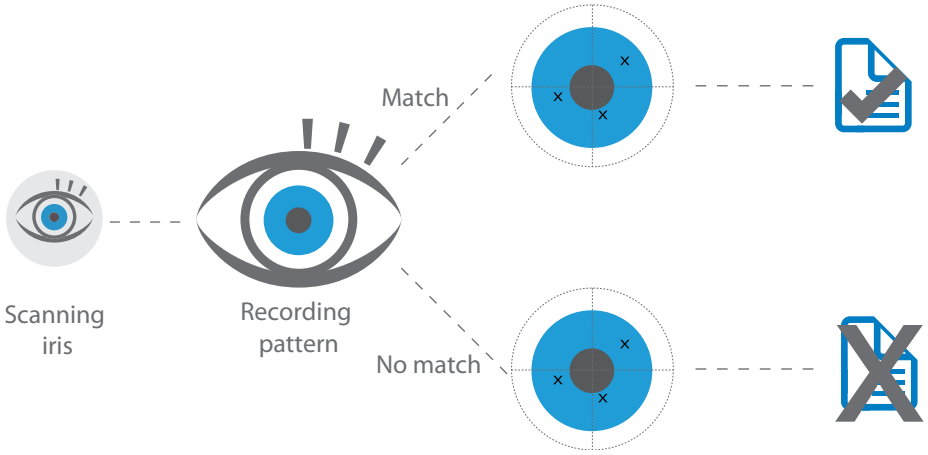
security systems to identify a unique user, promptly and conveniently. It requires installation equipment to recognize an individual. No physical contact is required between the individual and system during the authentication process. Even if the person wears glasses and contact lenses, the system functions normally since it does not change the characteristics of a person's iris. In fact, even when a person undergoes eye surgery, it has no effect on the iris.

The scanner reads from the outer iris inward. It plots different markings and maps the shape while recognizing the unique color of the iris based on markings. After recording the markings, the data is stored in a database for future verification. When the user accesses secure information, iris scanning is undertaken to match recorded patterns. The system grants permission if the user data matches, or else it gets rejected.

The Infosys Iris Scan Biometric Security Model

Banks can use an iris scan biometric security system to guarantee secure access of information and prevent security breaches. The system will ensure that information is accessed only by authorized persons. An iris scan biometric security system secures top secret documents by providing access only to users with unique attributes.

Our model proposes scanning the iris to verify the identity of the individual before granting access to banking information. When the user clicks to open the document, the scanner instantly scans the user's iris. The system matches the scanned image with template records. It also stores details of the user's last session. If the recorded scan matches the template of the authorized user, the document can be accessed. When the system does not authorize the user, it displays an 'unauthorized access' message.



The system uses a sensor to scan the iris and record patterns to be matched with the database for gaining access to documents. The scanning process is initiated every time a user seeks to open documents.

Our model can be implemented by banks where top secret information resides in documents. Banks cannot afford a security breach that has the potential of causing severe damage. The opportunity cost may seem prohibitive since the device and installation costs are significantly higher than traditional security systems. However, the upfront cost serves to insure top secret information from crippling losses. Moreover, the widespread adoption of biometric technology will lower the cost of devices and installation. When biometric security goes mainstream in banking, and

Advantages

1. The highlight of biometric security is its uniqueness. The possibility of two users having the same identification features in the biometric system is virtually zero.
2. The highly secure process of identifying users makes it less prone for users to share highly confidential information.
3. Biometric details of individuals cannot be stolen, forgotten or lost. Consequently, identification and granting access to authorized users is safe.
4. Biometric identification delivers extremely accurate and secure access to information. Fingerprints, and retinal and iris scans produce unique data sets.
5. An individual's identity can be verified without resorting to documents that may be stolen, lost or altered.

Disadvantages

1. Fingerprints as a method of identification is not feasible if an individual's hands are damaged due to an accident.
2. Individuals express concerns about eyesight due to scanning of the iris.
3. High cost of installation of devices for biometric security.

devices are available within a reasonable budget, it can be used for documents with lower levels of confidentiality.

Let Us Evaluate the Pros and Cons of Biometric Security Technology:

A robust security solution blends cryptographic functions, biometric security matching, feature extraction, and a biometric sensor in one device. The unified device offers protection of the secret / private key since biometric data as well as the secret / private key operate within the secure device.

Biometric authentication serves as an additional security cover. Low-cost and simple biometric security solutions enhance system security when used alongside existing traditional authentication methods.

Conclusion

Banks must protect sensitive data, avoid a security breach and prevent unauthorized access. Even a single instance of unauthorized access to secure data can cause significant loss of business and reputation. Documents classified as 'top secret', 'secret' and 'confidential' demand high-level security scanning and clearance. Banks must ensure that sensitive data is accessible only to authorized persons.

In traditional security systems, access to documents can be secured with limited network access and at the document level via passwords for documents and encryption of data. Password protection and encryption techniques do not guarantee data security. In addition, it does not ensure that the person is authorized to access information.

Biometric technology offers enhanced security while being convenient to use. It guarantees that information is accessed only by authorized persons. The security system offers a reliable method for authenticating users. It is a robust solution to meet the stringent requirements of restricted access for top secret information. Significantly, it reduces frauds and minimizes password administrator costs.

As biometric sensors become miniaturized and less expensive, biometrics will emerge as an effective strategy to protect information, safeguard privacy and prevent fraud. When biometric technology goes mainstream, banks can use biometrics in every transaction requiring the authentication of identity. Users may be authenticated by a workstation during login, by a smartcard to unlock the private key, or by a physical access control system to open a door. A biometric system can be deployed in all these areas to minimize unauthorized access, and consequently, business risks.

About the Authors

Mohan Kumar

Group Project Manager, Product, Research and Development group, Infosys

Mohan has rich experience in financial application development. He has global IT experience in the financial services and mobility industries and has a sound understanding of product and platform development. His areas of specialization include product and solution development, and process efficiency by leveraging IT and operational convergence in the financial and mobility domains. Mohan works on intellectual property creation, diverse projects under the 'Building Tomorrow's Enterprise' (BTE) initiative, and the development of banking applications.

Mohan can be reached at mohan_kumar08@infosys.com

Rakhi Agrawal

Technical Manager, Product, Research and Development group, Infosys

Rakhi has 13 years of experience in financial application development and project management. She is a specialist in product and solution development in the financial domain. She is developing a trading platform

Rakhi can be reached at rakhisinghal@infosys.com

Dhruv Chauhan

Product Technical Lead, Product, Research and Development group, Infosys

Dhruv has seven years of experience in application development in the conferencing and telecom domain. He is working on a trading platform development for web and mobile.

Dhruv can be reached at dhruv_chauhan@infosys.com

LinkedIn: http://www.linkedin.com/in/dhruvchauhan and Twitter: @dhruvchauhan

For more information, contact askus@infosys.com

Stay Connected