

**MSEP - 028**

SECURITY ANALYSIS FOR DIFFERENT PRODUCTS AND LEGAL AND TECHNICAL VERIFICATION FOR MORTGAGE SYSTEM AT HDFC BANK LIMITED

**SUBMITTED BY: SHILPA SINGH**

**ENROLLMENT NO: 2001436395**

**Submitted to the School of Vocational Education and Training,**

**IGNOU in partial fulfilment of the requirements**

**for the award of the degree**

**PG Diploma in Information Security (PGDIS)**

**Year of Submission-2020**

**A picture containing logo

Description automatically generated**

**Indira Gandhi National Open University**

**Maidan Garhi, New Delhi – 110068**

**CERTIFICATE OF ORIGINALITY**

This is to certify that the project report entitled **“Security Analysis for different products and Legal and Technical verification for Mortgage System at HDFC Bank Limited”** submitted to **Indira Gandhi National Open University** in partial fulfilment of the requirement for the award of the degree of **PG DIPLOMA IN INFORMATION SECURITY (PGDIS),** is an authentic and original work carried out by me.

The matter embodied in this project is genuine work done by me and has not been submitted whether to this University or to any other University / Institute for the fulfilment of the requirements of any course of study.

………………………. Signature of the Student

Date: 29th Dec 2020

Name and Address of the student

SHILPA SINGH

HOUSE NO 973 SECTOR-05,

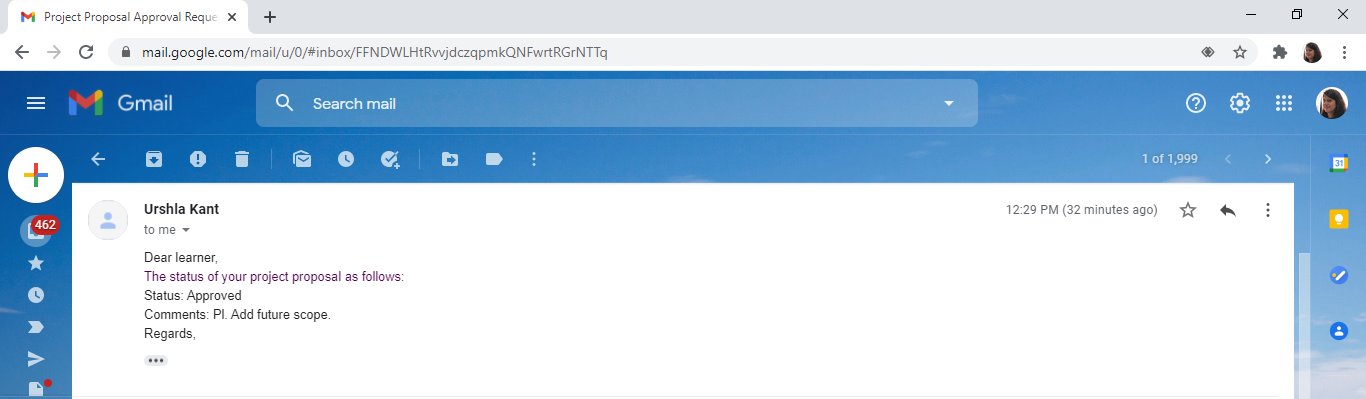
VASUNDHARA, GHAZIABAD

UTTARPRADESH

PINCODE-201012

Enrolment No. **2001436395**

**NOTE: -** Project Proposal Approval Mail Screenshot has been attached with this Proforma.



**SCHOOL OF VOCATIONAL EDUCATION AND TRAINING, IGNOU, MAIDAN GARHI, NEW DELHI – 110 068**

**II. PROFORMA FOR THE APPROVAL OF PGDIS PROJECT PROPOSAL (MSEP-028)**

***(Note: All entries of the proforma of approval should be filled up with appropriate and complete information.***

***Incomplete proforma of approval in any respect will be summarily rejected.)***

## Enrolment No.: 2001436395

**Project Proposal No :……………..**

***(for office use only)***

**Study Centre: 39026**

**Regional Centre: Noida RC Code:…39… E-mail: rcnoida@ignou.ac.in**

**Mobile/Tel No.: 9958-1402-89.**

1. Name and Address of the Student **SHILPA SINGH**

HOUSE NO 973, SECTOR-05, VASUNDHARA, GHAZIABAD. (U.P) PINCODE-201012

2. Title of the Project “**Security Analysis for different products and legal and Technical and verification for mortgage system at HDFC Bank”**

Signature of the Student Date: **29th Dec 2020**

**For Office Use Only**

…………………………………… Signature, Designation, Stamp of the Project Proposal Evaluator

Approved Not Approved Date: …………………….

**Suggestions for reformulating the Project:**

Ensure that you include the following while submitting the Project Proposal:

ACKNOWLEDGEMENT

As successful realization of the project is an outcome of consolidated effort of people from distinguished fronts. It’s only with their support and guidance the Candidate could meet the end. I am thankful to almighty without whose support I could not have completed this project.

First of all, I would like to thank HDFC Bank Ltd, for providing me an opportunity to work with them and develop a Business solution for them. The support and valuable time provided to me during my project was more than what anyone would have expected in such a domain.

My sincere gratitude goes to my Guide Ms. Anshu Bhaduri who guided me throughout the duration of my project & has rendered his helping hand, in form of motivation and criticism. He has imparted Functional Knowledge of Mortgage Loans, in spite of his hectic schedule as well, as and when required.

I am thankful to my Colleagues & Family members who have equally contributed time to time with their inputs, motivational words and helped me in collecting information about the Project

***“Shilpa Singh”***



|  |  |
| --- | --- |
| **S. No.** | **Topic** |
| 1 | Introduction |
| 2 | Company Profile |
| 3 | Problem Statement |
| 4 | Objectives of the study |
| 5 | Hypothesis of the study |
| 6 | Research Methodology |
| 7 | Limitations of Study |
| 8 | Theoretical Perspective |
| 9 | Legal and Technical Verification System of Mortgage Loans |
| 10 | Cryptography and its techniques |
| 11 | Cryptography implementation in Legal and Technical Verification of Mortgage Loans |
| 12 | Case Study |
| 13 | Conclusion and Recommendation |
| 14 | Future Scope |
| 15 | Questionnaire |
| 16 | Bibliography |

1. **INTRODUCTION**

This Project is based on understanding the concepts of security analysis for different Line of Business and Legal and Technical Verification for Mortgage System with respect to HDFC Bank Ltd. Security is one of the major factor considering sanctioning of Mortgage Loans. Legal and Technical Verification of mortgage loans cannot be done by each and every person of HDFC Bank , hence the link will be available for such verification only to employees having Sanctioned Limit. If we do not put any restrictions on accessibility of link, then there are chances of fraud detection. The user needs to take necessary precautions to prevent unauthorized and illegal use of access. User is also responsible for correctness of information supplied to HDFC Bank. This study will help HDFC Bank in determining and calculating the various financial reports and eligibilities for different product lines at HDFC Bank.

**Different product lines at HDFC Bank:**

There are various product lines which are used in HDFC Bank and information security for each and every loan is required without any compromise.

1. **For Commercial Vehicle Product,** calculation of various Data Analysis Sheets such as, Depreciation Grid Value (DGV), Principle Outstanding Sheet (POS), Fleet Calculator, Financial Summary Sheets, Ratio Analysis etc. in the system. Install a trusted antivirus such as Norton, Avast or McAfee and implement cryptographic techniques to protect the data which is vulnerable to being exposed.
2. **For Auto and Personal Product,** Customer’s Eligibility, FOIR Calculation etc. All these data calculation should be encrypted.
3. **For Mortgage Product,** Challenges pertaining to Legal and Technical verification of Property and Approved Project Finance (APF) for Mortgage Loans is currently catered from outside the system, so data coming from outside the system should meet various security parameters.

For security of above mentioned products, there are various security concerns which should be considered during all these product lines. These are:

1. Financial service institutions provide dynamic access to data for their clients. Such a high flow of information makes it difficult to protect data.
2. Social networking sites are also being used for advertisement of loans, and also these sites are inexpensive method of marketing financial products/services, hence, maintaining it difficult for maintaining the data security.
3. Cyber criminals are increasing day by day and they designed various techniques to outsmart traditional data security technologies.
4. Educating employees play an integral part in avoiding data leaks and handling sensitive data.

1. **COMPANY PROFILE**

HDFC Bank Limited is an Indian banking and financial services company headquartered in Mumbai, Maharashtra. It has a base of 104,154 permanent employees as of 30th June, 2019. HDFC Bank is the India’s largest private sector bank by assets. It is a largest bank in India by market capitalization as of March, 2020.

Full name of HDFC Bank is “**Housing Development Finance Corporation”.**

HDFC Bank was incorporated in 1994, with its registered office in Mumbai, Maharashtra, India. Its first corporate office and a full-service branch at Sandoz House, Worli were inaugurated by the then Union Finance Minister, Manmohan Singh.

As of 30 June, 2019, the bank’s distribution network was at 5,500 branches across 2,764 cities. The bank also installed 430,000 POS terminals and issued 23,570,000 debit card and 12 million credit cards in FY 2017.

HDFC Bank provides a number of products and services including wholesale banking, retail banking, treasury, auto loans, **mortgage loans**, two-wheeler loans, personal loans, loan against property, consumer durable loan, lifestyle loan and credit cards.

As of 30 June 2019, the **Bank's** distribution network was at 5,500 **branches** across 2,764 cities. **HDFC Bank** has over 2952 **ATMs** in **India.**

In March, 2020, HDFC made an investment of Rs.1000 crores in Yes Bank.

***VISION OF HDFC BANK***

"To become the market leader in Housing Development Finance in Sri Lanka"

***VISION OF HDFC BANK***

We define our mission in the broader context of our shareholders, customers, staff, the national economy, regulators and the natural environment.

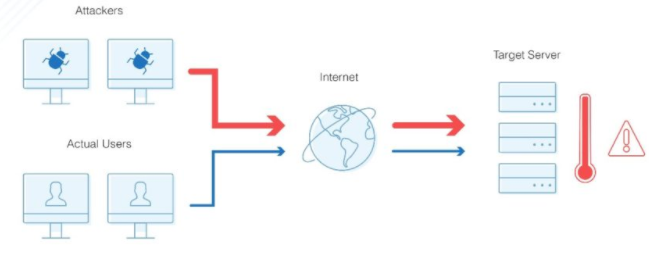
* To our shareholders, our mission is to optimize returns.
* To our customers, our mission is to provide a caring service by anticipating their requirements and innovatively satisfying them beyond their expectations.
* To our staff, our mission is to identify their multi-faceted talents, develop, motivate, recognize and reward them towards fulfilment of the institutional and national housing vision.
* To the national economy and the industry regulator, we are the key driver and thought leader, shaping and financing the national housing policy.
* To our natural environment, we enforce sustainable practices across all our activities.

**Area of study:** Ghaziabad, Noida

1. **PROBLEM STATEMENT**

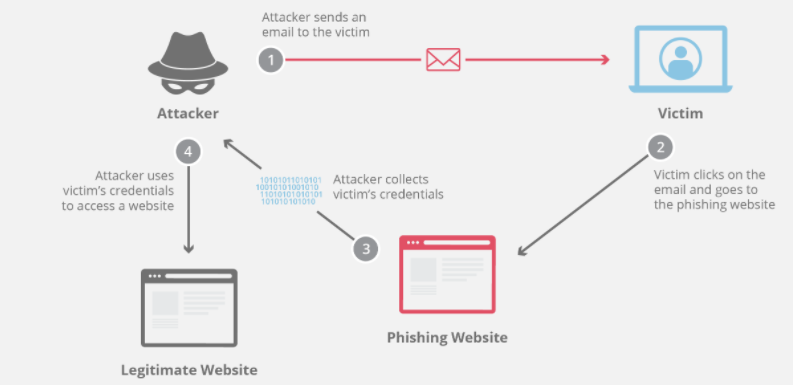
In today’s world, while technology and internet have made banking more convenient, but is also brings many security challenges. The number of cases of bank frauds are rising every year. Some of the major bank security issues are:

* **DDos Attacks**: This is Distributed Denial of Service Attacks. The perpetrators will hack the bank online system and database with a large number of requests and transactions which adversely affects the bank servers hence making the complete system slow so that bank user cannot avail any of the bank’s services.



**DDos Attack**

* **Phishing** is also very serious concern in terms of seeking for a loan. Fake emails or messages with attractive offers encourage consumer to click on a link to avail loan. It will encourage them to fill a form with their complete financial details and user’s all sensitive financial details will be exposed in wrong hands.

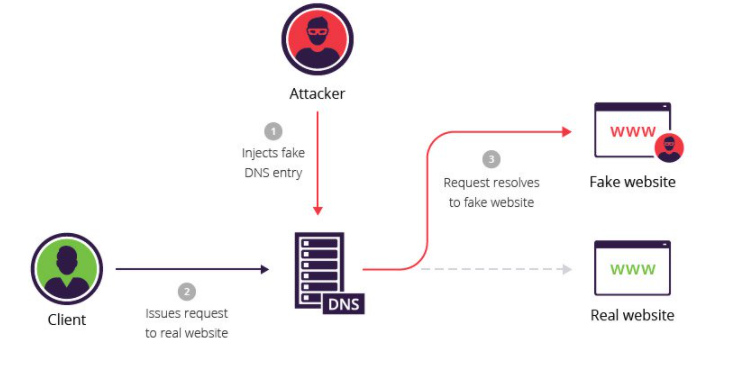


**PHISHING**

* **Spoofing** involves making a fake website of a bank which uses same color schemes, logo and pictures to mimic an original bank page. Customer when goes to fake page for applying loan, he/she enters its details and password that website will capture. Hence, fraudsters will use those details and rob the customer. **Spoofing** can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack

There are various types of spoofing:

* Email Spoofing
* Called ID spoofing
* GPS Spoofing
* Website Spoofing
* IP Spoofing
* Text Message Spoofing



**SPOOFING**

1. **OBJECTIVES OF THE STUDY**
2. As Mortgage Loans is very vastly handled in HDFC and has many extensive variants such as Loan Against Property, Home Improvement etc., so Legal and Technical Verification requirements would be a part of this study.
3. To study how Cryptography secure sensitive financial information by creating algorithms and ciphers to encrypt data. Hence, in order to secure all the transactions during the entire loan process, cryptography plays an important role.
4. To maintain the authencity of user accessing the system.
5. To ensure that no one can read the sensitive financial data accepts the intended receiver.
6. Ensuring that financial parameters of loan received by intended person has not been altered in any way from the original.
7. Study involves the mechanism to prove that data received by bank is actually sent by sender.
8. **HYPOTHESIS OF THE STUDY**

* The importance of information and the consequences of losing it will be evaluated.
* The hazard involved in safeguarding the classified information will be assessed.
* The method of preventing attackers from stealing information from computers pertaining to end user.

1. **RESEARCH METHODOLOGY**

This research is aimed at studying about the mortgage loans. Legal and Technical Verification is always involved in mortgage loans. Whenever bank sanctions a loan, these 2 verification are always involved and hence there is a risk of data breach, hence all the cryptographic techniques are involved also.

**Data Collection Methods:**

There are 2 types of sources from where data is collected:

1. Primary Source
2. Secondary Source
3. **Primary Source:** Primary data collection is done through surveys and interviews of bank employees.
4. **Secondary Source:** Secondary data collection is done through the data available already on various sources like internet, magazines, newspaper, books, journals, etc. Information already available needs analysis. Following are popularly used secondary search methods :

* **Data Available on the internet:** Oneof themostpopular way of collecting secondary data is internet. Website have a lot of information, and moreover no one has to pay for it, so people can download any amount of data without any limit. One main thing which we all should keep in mind is we all only use trusted website to collect information.
* **Public Libraries**: Public libraries are also a good source of secondary data collection technique. Public libraries generally have huge collection of books containing information about banking terminologies, banking products, marketing statistics, etc.

1. **LIMITATIONS OF STUDY**
2. The study of cryptography implementation in mortgages loans is limited to the areas of Noida.
3. In terms of Cryptography specific limitation, cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols and procedures.
4. Cryptography comes at cost as use of cryptographic technique requires setting up and maintenance of public key infrastructure requiring high financial budget.
5. **THEORITICAL PERSPECTIVE**

***Existing Lending System of HDFC Bank***

Product Description FinnOne™, product is a powerhouse of seamlessly integrated applications, designed to provide operational support, risk management and decision-making support to banks and financial services companies.

Finnone is a suite of financial software systems, designed to support the typical business offerings of lending institutions. This system provides solution for both asset as well as liability side of business, core financial accounting, and customer service. Customer Acquisition System, Loan Management System and Collections Management System are the major systems of FinnOne. It caters to loans, ranging from simple EMI backed retail finance to highly complex commercial lending scenarios. FinnOne™ focuses on both, retail and corporate loans, thereby emerging as a comprehensive solution to back any line of the lending business.

**The Customer Acquisition System (CAS)** is a web based system that fulfills the requirements of automating loan origination and application processing operations of a lending institution. LMS also focuses on the automation of various decision making functions, such as credit checking and underwriting.

**The Collections Management System (CAPS)** help you track and follow up delinquent cases and take actions to recover the due amount. The system manages the entire collection life cycle – from making soft calls to delinquent customers to taking legal action and repossessing the asset to recover the due amount.

**Loan Management System (LMS)** provides operational support to lending institutions for the asset side of their business, which is primarily driven by loans.

**This Finnone loan management** **system** caters for maintaining and tracking automates all stages of the loan origination and management life cycle right from entering details of the applicant to tracking the repayments and closing the loan. LMS caters to loan servicing requirements of any installment or non-installment based loan. The system allows creation of user definable and flexible accounting templates and maps them to the any accounting backend system. LMS optimizes repayment calculation and simulations methods for a variety of options, such as EMI, step-up and step-down, balloon and bullets, supports both fixed and floating interest rate types. LMS helps in performing the following tasks online.

1) Maintain loan details

2) Maintain a database of all the customers of the bank or lending institution 3) Process loan applications

4) Maintain disbursal details

5) Maintain post disbursal details

6) Print disbursal cheques

7) Generate repayment track record of the client

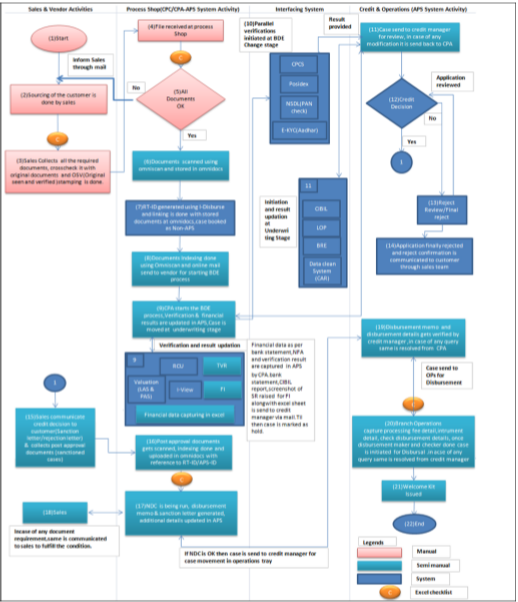
8) Maintain payable and receivable details automatically for each account

9) Securitize loans

**Current Business Flow Mortgage Loans in HDFC Bank**

Below is the current HDFC Business flow for the loans integrating the sourcing, Investigation and Processing agencies to smart credit decisions. It incorporates workflow and caters to the approval and deviation processes an organization may follow. This legacy system seamlessly integrates the various touch-points of the application origination systems of banks and financial services organizations in areas as credit appraisal need analysis, in-built deviation approval and integration to the lending system.

**WORKFLOW FOR MORTGAGE LOANS**



1. **LEGAL AND TECHNICAL VERIFICATION SYSTEM OF MORTGAGE LOANS**

A mortgage loan, or just mortgage, is used either by purchasers of real property to raise funds to buy real estate; or alternatively by existing property owners to raise funds for any purpose, while putting a lien on the property being mortgaged. The loan is "secured" on the borrower's property through a process known as mortgage origination. This means that a legal mechanism is put in place which allows the lender to take possession and sell the secured property ("foreclosure" or "repossession") to pay off the loan in the event that the borrower defaults on the loan or otherwise fails to abide by its terms.

Features of mortgage loans such as the size of the loan, maturity of the loan, interest rate, method of paying off the loan, and other characteristics can vary considerably. The lender's rights over the secured property take priority over the borrower's other creditors which means that if the borrower becomes bankrupt or insolvent, the other creditors will only be repaid the debts owed to them from a sale of the secured property if the mortgage lender is repaid in full first.

In many jurisdictions, it is normal for home purchases to be funded by a mortgage loan.

HDFC Home Loan, one of the largest Home Loan financiers in India, offers you multiple benefits, through some of the best home deals. From doorstep service to minimum paperwork, we offer you a completely hassle-free loan package. Choose from a variety of loans and meet your specific loan need.

Home Improvement Loan HDFC offers Home Improvement Loans to facilitate improvement of a self owned dwelling unit to existing or new customer.

Home Improvement Loan considers a range of facilities internal or external to the structure without increase in the living space like Painting, Renovation etc.

**Land Loan** A Land Loan provided by HDFC equips you with finance to buy a residential plot for constructing your home. The Land Loan can be financed only within municipal limits of pre-specified locations or in cases of direct allotment by the concerned development authority, outside municipal limits.

**Office Premises Loan** Office Premises Loan from HDFC Home Finance enables entrepreneurs to purchase, construct or extend your office premises. You can expand your business with ease and also satisfy your workforce through a well furnished office.

**EMI Under Construction** EMI Under Construction enables you to make payments through EMIs, in a partly disbursed loan for an under construction project. The loan amount is partly disbursed and EMI is set as per the sanctioned amount. The tenure of the loan keeps moving up with additional amount being disbursed. The EMI will remain constant during the tenure of the loan. Save on interest and ensure faster repayment of the loan. Since your EMI starts immediately after the 1st disbursement, your principal repayment also begins simultaneously, thereby reducing your interest burden and tenure.

**Balance Transfer** Transfer your outstanding loan easily with HDFC Home Finance Balance Transfer facility. This is a facility offering you a choice to transfer the outstanding balance of the loan availed from other banks/ Financial institutions for more favorable terms & conditions.

You can also increase the loan amount through a Top-Up Loan.

**Top-Up Loan** Access your Top-Up Loan as and when you need to meet your personal requirements (other than for speculative purposes). Benefit from some

additional funds against the security of your property. Access this loan for various personal requirements depending on the property value.

Home Loan Process Existing Process of Mortgage Loans at HDFC Bank is shown on Page no 22. Diagrammatic representation of the same is as below:



***Existing Individual Property Technical Verification Process Flow***

Below is the existing process of Technical Verification at HDFC bank which is done outside the system. Here we are merging the Technical Verification piece inside the Legacy Finnone System for Mortgages.

1) Customer submits property documents to sales person who then collects document from customer and initiates an Individual Technical Request after logging into System.

2) Sales person fills in basic information pertaining to property and submits the request and Unique Request Id is created in system.

3) A technical admin user can see the respective request on dashboard.

4) Technical admin user can take a decision as to accept or deny the request basis completeness of request in terms of available documents.

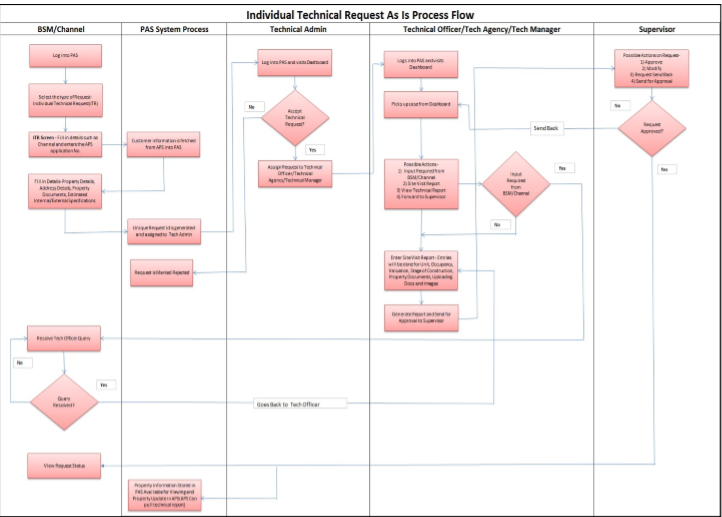
5) If technical admin has accepted the request then he/she assigns the request to either internal technical team employee or external technical agency.

6) Technical agency/ technical team employee visits the site and submits the site visit report.

7) Technical agency/technical team employee updates the site visit report into system and submits to technical team supervisor for approval.

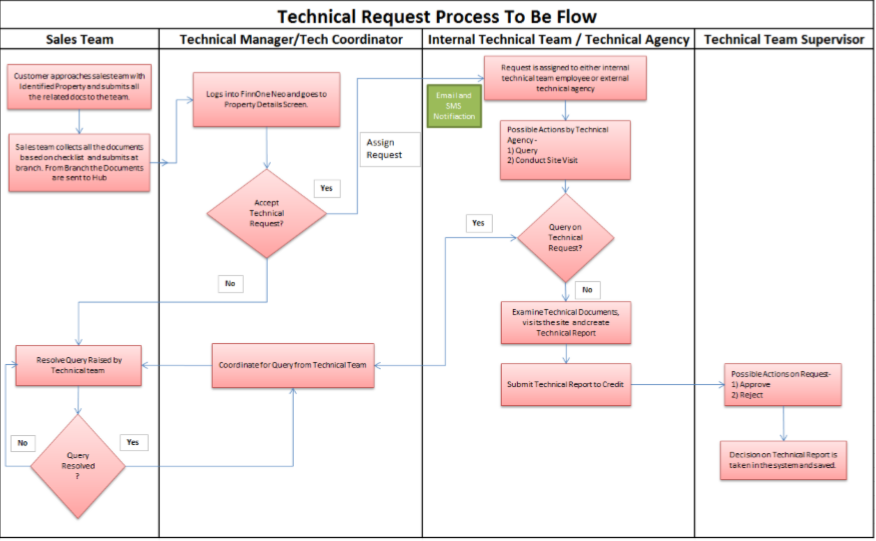
8) Technical team supervisor logs into system and takes a decision on the technical report.

9) Query mechanism within system is available to keeping a track on clarifications raised at any stage.



**HDFC Bank Technical Verification Process**

In the proposed system design, all the Masters would be independent and maintained in one system. Since this is a single system there would be no chances of any connection related issues as well. There will be a change in the process of Technical verification in Mortgage loans with the existing As is Process of HDFC Bank. Below is the newly designed Process Flow which will squeeze the process and thus results in faster processing of Documents.



In the proposed system design, all the Masters would be independent and maintained in one system. Since this is a single system there would be no chances of any connection related issues as well. There will be a change in the process of Technical verification in Mortgage loans with the existing As is Process of HDFCBank. Below is the newly designed Process Flow which will squeeze the process and thus results in faster processing of Documents.

***Existing Individual Property LEGAL Verification Process Flow***

Following is the process for legal verification for Bank:

* CPA : Credit Processing Agent
* BSM : Branch Sales Manager
* BCM : Branch Credit Manager

1) Customer submits property documents/sales person collects document

2) Credit Processing Agent (CPA) submits the request for legal verification in system.

3) CPA enters basic details such as property information, property address, document checklist and selects the lawyer to whom case is to be allocated

4) Unique Request Id is created in system and assigned to lawyer.

5) Lawyer is in parallel notified over email of the case and documents are sent to lawyer through courier. Lawyer can have query with respect to documents submitted. Lawyer can raise a query to the CPA in system. BSM acts on ground to clarify the query and CPA forwards the response to Lawyer.

6) Lawyer can login into system and submit and upload report. However practically lawyers submit report mostly in hard copy.

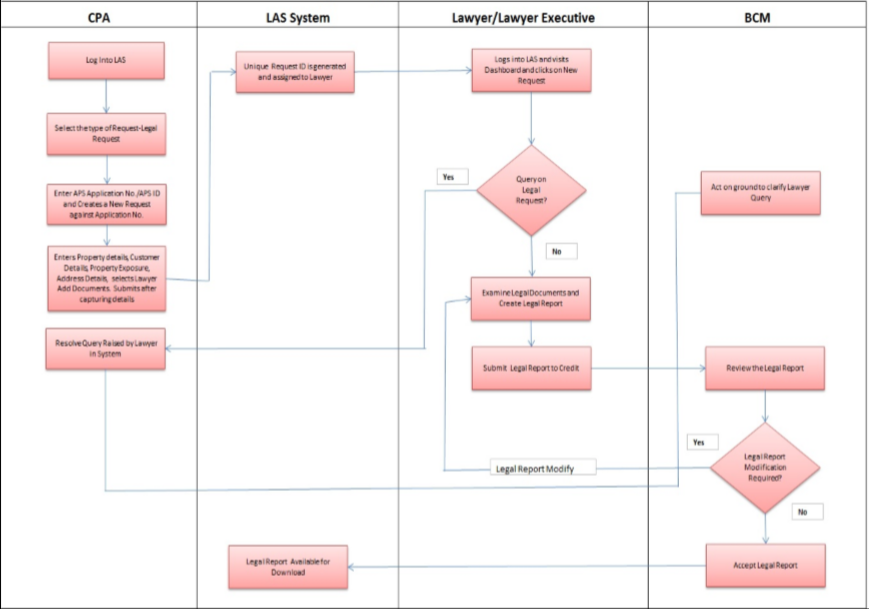
7) CPA/Lawyer executive updates legal report into system and submitted for credit review.

8) BCM may have query on the legal report. BCM can raise query to Lawyer on system. CPA acts on the query raised by BCM and liaisons with Lawyer to get the query clarified. CPA updates the query response on behalf of lawyer into system.

9) Once BCM is ok with report, BCM/respective credit user approves the legal report.

10) Query mechanism within system is available to keeping a track on clarifications raised at any stage.

Given below is the diagrammatic representation of legal verification process for HDFCBank in existing System

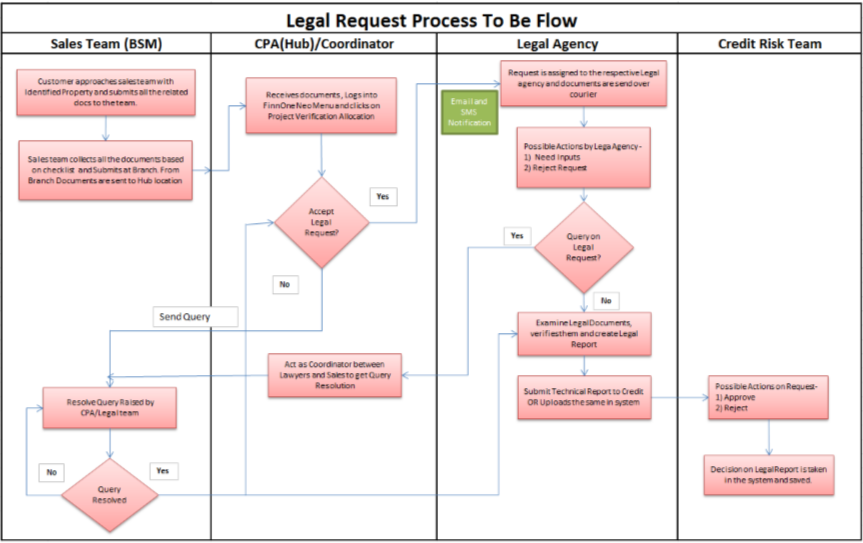


**HDFCBank Legal Verification Process**

In the proposed system design, all the Masters would be independent and maintained in one system. Since this is a single system there would be no chances of any connection related issues as well.

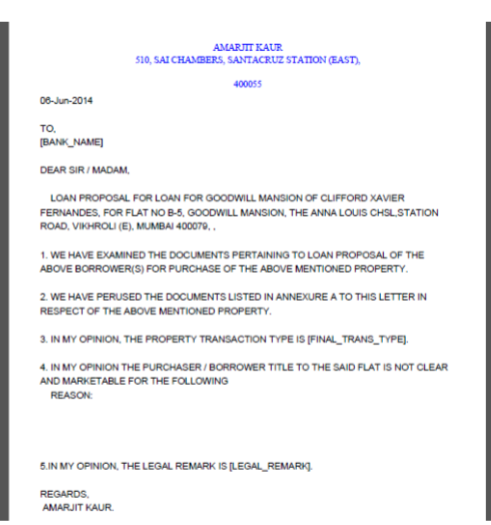
There will be a change in the process of Legal verification in Mortgage loans with the existing. As is Process of HDFC Bank. Below is the newly designed Process Flow which will squeeze the process and thus results in faster processing of Documents.

Given below is the diagrammatic representation of the Individual Legal Verification to be process in HDFC Bank.



**Legal Verification To be Process**

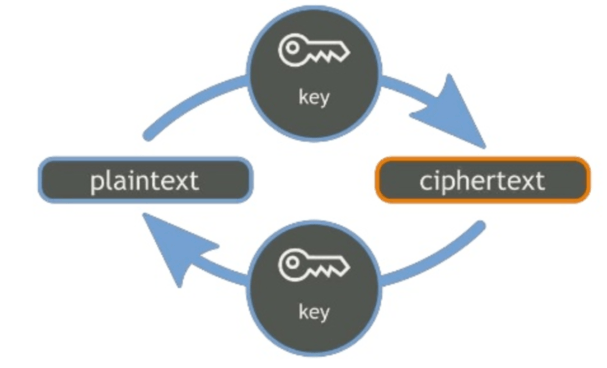
***Sample Lawyer Report***



1. **CRYPTOGRAPHY AND ITS TECHNIQUES**

Cryptography is a technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “**crypt**” means “**hidden**” and suffix **graphy** means “**writing**”.

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used.



**CRYPTOGRAPHY**

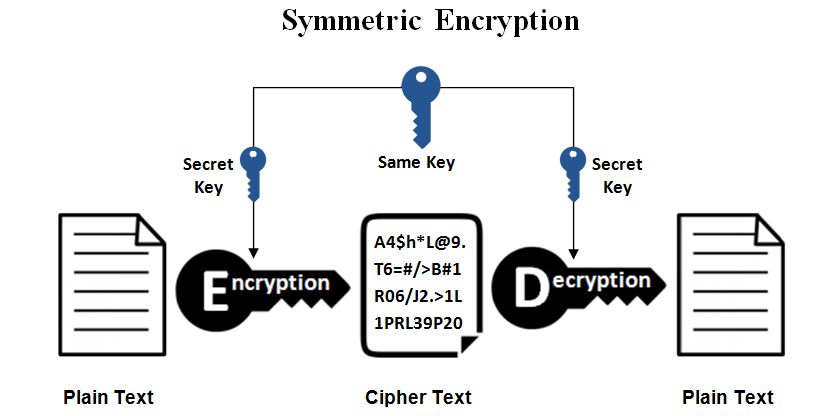
**Features of Cryptography are as follows:**

1. **Confidentiality :** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

**Types of Cryptography:**

1. **Symmetric Key Cryptography :**

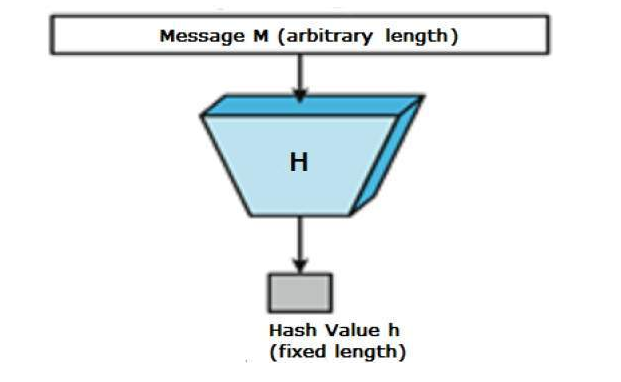
It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).



**SYMMETRIC KEY CRYPTOGRAPHY**

1. **Hash Functions :**

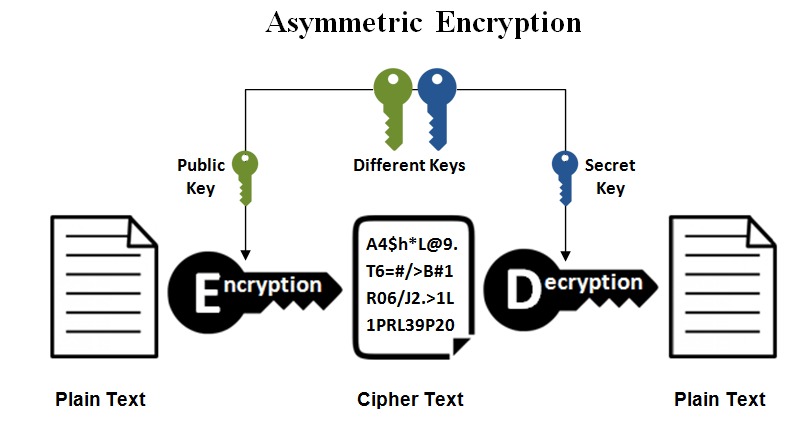
There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.



**HASH FUNCTIONS**

1. **Asymmetric Key Cryptography :**

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.



**ASYMMETRIC KEY CRYPTOGRAPHY**

1. **Cryptography implementation in Legal and Technical Verification of Mortgage Loans**

**Cryptography** is the study of abstracting information from undesired users of the same. **Cryptography** techniques have long been **used** in the **banking** industries to ensure the security of monetary transactions including the security of ATM cards, computer passwords, electronic commerce and loans sanctioning.

The development of cryptographic techniques has seen a lot of applications in the banking industry. If we talk about the **mortgage loans**, it is highly used in sanctioning a bank loan. There are various steps during the loan flow which requires data security at each and every step and financial data is very sensitive to be exposed. It has various parameters like Customer Personals details, Customer demographic details, PAN Number, income details, loan parameters, etc.

***Security implementation in Mortgage Loan Flow:***

1. First step is, sourcing of loan is done. It is done either by HDFC Bank application or by third party. There are many 3rd parties which sources loan, for eg., Bank Bazaar.

Bank Bazaar collects data from the customer who visited their site and shows their interest of getting a loan. 3rd party when share customer data to HDFC bank, that data is first encrypted by **AES algorithm** while transferring over the network and then it reaches to bank database.

1. After sourcing of a loan is completed, sales collect all the documents of a customer which are required to sanction a loan and crosscheck all with their respective originals and hence original seen and stamping is done. All these documents are also **password protected**, so if by any case documents landed into wrong hands then also they cannot be misused.
2. File is now received at Process shop for loan documentation.
3. When all documents are cleared as OK, then these documents are stored in Omnidocs system in encrypted form. Omnidocs is a centralized system which stores all the documents.
4. RT-ID is generated and linking is done with stored documents at Omnidocs and case is booked.
5. Documents indexing is done using Omniscan and online mail is send to Vendor for starting Basic data entry (BDE) process.
6. Credit processing authority starts the BDE process, Verification and financial results are updated in APS and then case is then moved at underwriting stage. Underwriting stage is a stage at which Credit Manager approves the loan after verifying all the parameter required for a loan.
7. There are various types of verification which are required during loan sanction :



**RCU**: Data verification is done through 3rd party.

**TVR**: Tele verification is done from customer.

**Valuation (LAS & PAS):** Legal and Technical verification is done.

**In Legal verification,** data is send to lawyer to an agency which is registered with HDFC bank. Here, while sharing the data to 3rd party, all the data is encrypted using a key. Same key is also used by 3rd party to decrypt the data.

**In Technical verification,** data is send to technical agency for technical aspects of verification. Here, while sharing the data to 3rd party, all the data is encrypted using a key. Same key is also used by 3rd party to decrypt the data.

1. NDC is run, disbursement memo and sanction letter is generated.

Additional details updated in APS. If NDC is OK, then case is send to credit manager for case movement in operations tray.

1. Simultaneously, CPCS, POSIDEX, NSDL (PAN check), CIBIL, BRE and EKYC is done as a part of loan process.
2. If all these verifications are completed, then case is sent for reviewal.
3. Post approval documents are now submitted by customer.

***Detailed Description of Cryptography in Banking***

The development of cryptographic techniques has seen a lot of applications in the banking industry. This whitepaper focuses on the review of the major cryptographic techniques which has been used extensively in the banking industry, for the implementation of data security norms and the fulfillment of compliance requirements. While techniques have not been described in details, the focus has been on exploring the business implications of these developments.

Cryptography is the study of abstracting information from undesired users of the same. Cryptography techniques have long been used in the banking industries to ensure the security of monetary transactions including the security of ATM cards, computer passwords, loan disbursement to account and electronic commerce. Until modern times, cryptography referred almost exclusively to encryption, the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., cipher-text).

***Decryption*** is the reverse, moving from unintelligible cipher text to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. Some more popular methods used in cryptology in the financial institutions like banks are public-key cryptography, symmetric-key cryptography and triple DES cryptography.

Cryptography tries to ensure the following objectives through various techniques:

• **Authentication**: The process of proving one's identity.

• **Privacy/confidentiality**: Ensuring that no one can read the message except the intended receiver.

• **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.

• **Non-repudiation:** A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

**TYPES OF CRYPTOGRAPHY ALGORITHMS**

There are several ways of classifying cryptographic algorithms. For purposes of this study, they will be categorized based on the type of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are Public Key Cryptography (PKC), Symmetric Key Cryptography (SKC) and now use the Triple Data Encryption Standard (TDES). Banks started using cryptographic techniques using PKC at first, and then they started using SKC. SKC usage finally evolved to Triple DES from DES.

***PUBLIC-KEY CRYPTOGRAPHY OR ASYMMETRIC KEY CRYPTOGRAPHY***

Public-key cryptography is a method for secret communication between two parties without requiring an initial exchange of secret keys. It can also be used to create digital signatures. Public key cryptography is a fundamental and widely used technology around the world, and enables secure transmission of information on the Internet and was first embraced by banking institutions for sensitive data transfer operations. It is also known as ***asymmetric cryptography*** because the key used to encrypt a message differs from the key used to decrypt it.

In public key cryptography, a user has a pair of cryptographic keys — a public key and a private key. The private key is kept secret, while the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The keys are related mathematically, but the private key cannot be practically derived from the public key.

The two main branches of public key cryptography studies are:

* **Public key encryption** — a message encrypted with a recipient's public key cannot be decrypted by anyone except a possessor of the matching private key -- presumably, this will be the owner of that key and the person associated with the public key used. This is used for confidentiality.
* **Digital signatures** — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender had access to the private key (and therefore is likely to be the person associated with the public key used), and the part of the message that has not been tampered with.

A major advantage of using public key encryption is the ease of distribution of the keys. These public keys may be used for distributing subsequent keys, or for protecting data communicated between devices. In a network of n cryptographic devices, on the order of n2 initial keys are needed in order for all pairs of devices to communicate securely. The most conventional method for distributing the keys has been via manual delivery such as with trusted couriers. This is generally not cost-effective for a large network consisting of thousands of cryptographic devices. With public key cryptography, electronic distribution of initial keys is more feasible and economical using a simple, widely known protocol. For the banking industry, especially in retail banking, this is highly effective, when the number of customers is often large and geographically dispersed. When a device wishes to establish a secure channel, it first generates a public and private key pair. The public key is sent to the intended receiving device on the open communication channel, and the private key is retained by the generating device. On receipt of the public key, the receiving device encrypts an initial DEA key-encrypting key with the public key and sends the encrypted key value to the originating device. Since the private key is known only to the originating and only this device can decrypt the encrypted initial key encrypting key to establish a secure communication session with the other device. Various methods have been proposed for certifying and registering public keys, and for improving the integrity of the key distribution process.

First, with public-key-based key distribution, the certification center or the authentication server can be off line and key distribution is still possible. In contrast, with secret-key-based key distribution, on-line access to a key distribution center is usually needed each time the communicating parties establish an initial keying relationship. Second, in public-key-based key distribution, the degree of trust placed on the central authority (e.g., a certification center) is generally less than the degree of trust placed on the central authority in secret-key-based key distribution. With public key cryptography, electronic distribution of initial keys is more feasible and economical using a simple, widely known protocol. Public key cryptography is also well-suited to the digital signature mechanism that supports non-repudiation applications, which are applications that can establish the authenticity of an originator of a message or data. The RSA algorithm, which uses a variable size encryption block and a variable size key, is the first and most common algorithm that was used for encryption in the banking industry.

***SECRET-KEY CRYPTOGRAPHY OR SYMMETRIC KEY CRYPTOGRAPHY***

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption. In symmetric-key cryptography, the plain text is encrypted by mangling it with a secret key. Decryption requires knowledge of the same key, and decryption reverses the mangling. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

Other terms for symmetric-key encryption are secret-key, single-key, shared-key, one-key and eventually private-key encryption.

Symmetric-key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits are commonly used for encryption processes when high security concerns rule rather than computational intensity. The Advanced Encryption Standard algorithm approved by NIST in December 2001 uses 128-bit blocks.

Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms. In practice, asymmetric key algorithms are typically hundreds to thousands times slower than symmetric key algorithms.

One disadvantage of symmetric-key algorithms is the requirement of a shared secret key, with one copy at each end. In order to ensure secure communications between everyone in a population of n people a total of n(n − 1)/2 keys are needed, which is the total number of possible communication channels. To limit the impact of a potential discovery by a cryptographic adversary, they should be changed regularly and kept secure during distribution and in service. The process of selecting, distributing and storing keys is known as key management, and is difficult to achieve reliably and securely. Public distribution need manual delivery of keys by a reliable agent, and as such is a cost intensive operation.

In modern cryptosystems designs, both asymmetric (public key) and symmetric algorithms are used to take advantage of the virtues of both. Asymmetric algorithms are used to distribute symmetric-keys at the start of a session. Once a symmetric key is known to all parties of the session, faster symmetric-key algorithms using that key can be used to encrypt the remainder of the session. This simplifies the key distribution problem, because asymmetric keys only have to be distributed authentically, whereas symmetric keys need to be distributed in an authentic and confidential manner.

Symmetric ciphers have historically been susceptible to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis and linear cryptanalysis. Careful construction of the functions for each round can greatly reduce the chances of a success of attacks.

***TRIPLE DATA ENCRYPTION STANDARD OR TRIPLE DES***

This Data Encryption Standard is a method for encrypting information that is based on a Symmetric-key algorithm that uses a 56 bit key. DES is considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small. DES consequently came under intense academic scrutiny which motivated the modern understanding of block ciphers and their cryptanalysis. This led to the development of Triple DES. These algorithms are essentially symmetric encryption techniques only, only modified to support greater security concerns.

Triple DES is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times. In general TDES with three different keys (3-key TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3-key TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits.

When it was found that a 56-bit key of DES is not enough to guard against brute force attacks, TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. The use of three steps is essential to prevent meet-in-the-middle attacks that are effective against double DES encryption.

TDES can be operated with variations in two parameters: number of keys used and order of operations.

In general TDES with three different keys (3-key TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3-key TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. A variant, called two-key TDES (2-key TDES), uses k1 = k3, thus reducing the key size to 112 bits and the storage length to 128 bits. However, this mode is susceptible to certain chosen-plaintext or known plaintext attacks. The best attack known on 3-key TDES requires around 232 known plaintexts, 2113 steps, 290 single DES encryptions and 288 bits of memory, which given the current computational development, is impossible. Today most of the banking transactions use TDES encryption because it is not possible to crack the key of TDES given the current stage of developments in computation speed and capabilities.

1. **CASE STUDY**

The importance of banking online has grown enormously in the past decade. Making for more profit and better convenience it is not likely to fade away anytime soon. This also presents some new hurdles for the **online banking** community. As the number of banking online customers increases the amount of criminal attacker will also increase. The bank recognizes this trend and therefore to maintain and even grow customer confidence and trust they develop ways to keep the customer data and money safe. The bank has to take on an enormous feet which is to protect customers and staff from the attacker and themselves. The banking security is only as strong as the end user of the terminal machine or the end user/customer using a credit/debit card. Throughout this paper I will present key facts and issues of this case then I will go through these issues giving alternative solutions and engaging in the pros and cons of those solutions.

***KEYS FACTS***

* Operations for HDFC bank had first got up and running during the year 1995 of the month of January
* HDFC bank was one of the first banks to set up online banking.
* HDFC is a trusted name in banking, 2,544 branches, 9,333 ATMs, 1,399 towns & cities.
* HDFC Bank is one of the leading private banks in India
* HDFC identifies public key infrastructure, during PKI’s infancy, as a suitable technology to address security.
* In the Indian sector of banking there are basically 5 types of banks:
* Private sector banks
* Regional rural banks
* Foreign banks
* Co-operative banks
* Public sector banks.
* Once RBI had published the guidelines on internet banking HDFC started its online services.
* For internal risk management HDFC bank used technology-intensive models.
* The data center and backup systems where held at two different geographical locations in Mumbai.
* RBI guidelines report banks should utilize the outside experts known as ethical hackers to penetrate systems, inspect infrastructure, and test physical access controls
* HDFC has made the commitment to bring new products and attract new customers while signing with RSA security, the US based provider of IS solutions.

***KEY ISSUES***

**Key Issue 1:** Improving banks services to attract and keep new customers.

**Alternative Course Solution:**

* 1. Making the banking experience as fast and efficient as possible. Bringing up-to-date technologies to the front doors of the customer. State of the art website, phone applications and ATM’s will bring the banking experience to new levels.

**Pros:**

* By utilizing these channels of communication between the bank and the customer a very nice freeway of information exchange begins to take shape.
* This is a very effective way to monitor customer transactions and to weed out the unauthorized user.
* By Making the bank internet fast and secure, disbursement of loans has become very easier and fast. People can get the loans at the click of link and money gets disbursed very fast and in a safe manner.

**Cons:**

* At the same time tracking customers can be an issue. Unless an efficient, effective protocol is established to track customers through these various channels it could become a headache and very difficult to manage.
* To achieve a protocol that makes exchanging data over numerous channels work will endure cost. The adding of such protocol’s and policies will likely put the price tag higher.
  1. Taking an effective promotional stand will attract new customer and help boost the banks reputation helping to keep those customers.

**Pros:**

* Setting the stage with an effective promotional scheme will certainly attract and secure new customers
* When the customer numbers increase so shall the banks revenue stream. Bringing a happy bank and happy employees.

**Cons:**

* To develop and implement such a promotional scheme the bank will have to put out the money. Cost is always an issue when trying to improve you business.
* Reaching out to people and trying to attract new customers can back fire. If the promotion offends people, annoys people or if it is just done poorly then it could actually have the opposite effect and could eventually hurt the bank.
  1. By making use of website, phone app’s, ATM etc. . . . the bank can connect with the customer in a personal, effective way.

**Pros:**

* Pulling off this venture will build the relationship between bank and customer. The banks rep will grow and that is a very positive thing.
* Having all of these channels through which the bank customer can use will provide a sense of anytime banking. Online, no problem, on the phone, no problem, on the road, no problem.

**Cons:**

* If everything is not perfectly setup than the customer satisfaction rate will definitely suffer in which the bank will suffer.
* Ultimately by receiving a bad banking experience the bank could lose customers.

**Key Issue 2:** Through the banking authority how to maintain information security?

**Alternative Course Solution:**

a) Keeping the personal data, confidential data out of the hands of non-authorized personal.

**Pros:**

* Keeping sensitive information such as home addresses, telephone numbers, social-security numbers out of unauthorized hands will prevent fraud in credit, debit and account information.
* By maintaining the personal data in-house it will also make for a more informed staff making for a better service and more complete work force.

**Con:**

* This security measure could hurt relationships. The sharing of information if done correctly could actually build a relationship and by taking this out of the equation it could actually prevent a great binding.
* The fact that an employee may use the information for a sinister purpose will always be a concern. The bank has to do the best they can with this type of in-house problem.

b) Using a strategy that employ’s ethical hackers to attempt penetration on systems and network infrastructure.

**Pros:**

* Will give the bank an awareness on which system programs are vulnerable to attack.
* Maintaining all personal info: home addresses, social security numbers , credit card numbers and financial details of a customer.

**Cons:**

* By using ethical hackers the bank put its sensitive information out there. It gives up very sensitive information, its secrets so to speak.
* When bringing in outside help the bank also brings in additional expenses. To hire an ethical hacker the price tag could be very large. A salary for an ethical hacker shows the story.

c) Maintaining software by way of updating and personal training.

**Pros:**

* By testing and keeping watch of your systems the bank will achieve the ultimate efficiency.
* System programs, web applications, data servers etc. . . . all will be extremely enhanced.

**Cons:**

* As we found with employing ethical hackers the price tag will no doubt go up.
* It is also possible that by taking this route the deliberate modification of some admin tools could take place.

**Key Issue 3:** Continuity in business is essential, how to maintain it?

**Alternative Course Solutions:**

a) Backing up data, being able to recover if the need should ever arise.

**Pros:**

* By backing up data the bank ensures itself in times of natural disaster, robbery, and any other type of event that could otherwise cause the bank to lose precious personal data.
* The fact the banking organizations have such a spread of devices and applications, channels of communication between the public having data backed up can make for a well programmed system in which real time information is received in a more-timely manner.

**Cons:**

* Having information especially sensitive information always bring the possibility of the misuse of such data.
* The data will be stored on databases and SQL injections and other database driven attacks will be a real threat.
* The cost to ensure the correct safety measures and data systems will go up.

b) Making use of geographically locations, having more than one location.

**Pros:**

* Like other pro’s the bank can attract more and a new variety of customers by utilizing numerous bank locations.
* The range of people the bank will reach will increase thus bringing in new customers.
* By having more locations than the banking organization can spread. In doing this the bank will bring in better network connections and new and long lasting customers.

**Cons:**

* If the bank does decide to invest in new locations that is exactly what they will have to do, invest. Putting out more money to open new locations, staff, devices, new protocols all add up.
* Deciding where to put these new branches could also be time consuming and costly. If a bank location go through and does not work out it would be like a money pit for the bank.

**Key Issues 4:** What are the security challenges in online banking?

**Alternative Course Solutions:**

a) Making sure the customers data is stored safe and soundly.

Pros:

* If this is done correctly the bank will gain a respectable reputation and with this will develop more customers.
* Having this much data and the type of data that it is can make for some pretty exciting and state-of-the-art systems.

**Cons:**

* This is a task that is a lot easier said than done. If the security systems that are put into place to hold this data is not completely secure data theft could be a real possibility.
* Holding this much data will bring with it the cost factor. The more data and the more complex the system gets the more money will be needed to develop and implement a secure database system.

b) Keeping a close relationship with the customer, not relying too much on automated systems.

**Pros:**

* Making the effort to still provide a personal experience for the customer brings a sense that the bank cares and that they understand in a personal way.
* By keeping the personal connection with the banking customer the bank itself can tell what the vibe is on the back, hear what is trending, and basically have a view that is from the other side, the customer side.

**Cons:**

* It is possible that by building such close bonds between bank staff and open public banking customer the bank opens up the door to insider attack.
* Employees that might have a negative view on the bank could reveal trade secrets, banking data, or sabotage.

**Key Issues 5:** What are the challenges faced by Salvi?

**Alternative Solution Course:**

**a)** Making HDFC a “World class Indian bank”.

**Pros:**

* This is a respectable ambition and it definitely sets the bar.
* Under the watch of Salvi the customer should know that customer care and satisfaction will be at the highest priority.

**Cons:**

* Putting this type of standard in the mix could affect decisions, in turn the customer could suffer.
* To become a World class bank HDFC must transform the offline user to the online user. This is obvious but it is also a costly and very cumbersome project.

**b)** Securing Online Banking.

**Pros:**

* Without question making the hard transition from offline banking to online banking will create a more efficient better class of bank.
* If Salvi can make online banking secure than growing into the world class bank should follow.

**Cons:**

* Online banking brings new security risks: authentication, authorization, privacy, integrity, and non-repudiation.
* The higher the banks reputation might actually make it a target for criminal trying to make a name for themselves.

c) Reducing false positives

**Pros:**

* This would help to not bother the law abiding, everyday banker.
* Over time the false positives should work themselves out and the banking system will be greater for it.

**Key Issues 6:** Compulsions at HDFC Bank.

**Alternative Solution Course:**

**a)** Keeping customers in the automated channel. ATMS, online banking, mobile devices etc. . .

**Pros:**

* This will provide customers with better services. By keeping up-to-date with the state-of-the-art technologies the bank keeps efficiency at an all-time high.
* This can attract new customers they like the fact that they can do banking business from the safety of their homes.

**Cons:**

* The one-to-one bank teller to customer relationship gets forgotten about.
* Most Indian Bankers are familiar with the one-to-one banking, they like the personal service.

**b)** Increasing customers

Pros:

* The more customers the more money/revenue the bank will receive.
* Growth, gain, and prosperity are some key virtues of a bank and with this in mind HDFC should always be on top of their game.

Cons:

* Always promoting, reaching out to increase the customer rate the bank could lose focus on what their really there for.
* The more customers the more problems.

**Key Issues 7:** Roadmap the chief information officer (CIO) can implement.

**Alternative Solution Course:**

**a)** Secure the customer transition from offline to online banker.

**Pros:**

* This will grow the banks revenue, increase customers, making for a very efficient banking system.
* This has to be accomplish if Salvi will reach the ultimate goal of World Class Bank.

Cons:

* As is apparent phishing scams will come to light.
* With the online banking operation comes more security issues.
* Lose the personal relationship between customer and staff.

**b)** Secure online banking.

**Pros:**

* The online banker will feel more comfortable when doing business online.
* This is a step in the direction to become a world class bank.
* Will bring more with it a better reputation and more customers.

**Cons:**

* The cost will always be a negative aspect of any progress.
* With the online banking even if it is considered secure the criminal element will be more of an issue.

**c)** Evolve into the world class bank

**Pros:**

* This is the goal that Salvi wishes to reach and it is a prestige’s accomplishment.
* With this comes the attention to detail, finer service a World Class elegance.

**Cons:**

* With this with also bring the increasing of hardware and software maintenance, upkeep of websites, management of data centers.

1. **CONCLUSIONS AND RECOMMENDATIONS**

Based on the study of Security Analysis of Mortgage Loans at HDFC Bank, below are the conclusions:

***Conclusions:***

* We have identified that while sanctioning a loan to Customer, there are many sensitive personal, income and financial details of a customer which are vulnerable to be exposed. After implementation of the proposed Solution and applying Cryptography, HDFC would be able to overcome its pain areas and thus could improve on its security to securely disburse the Mortgage Loan to the customer.
* We have analyzed the challenge with respect to Mortgage loans wherein there are different systems for loan origination and Legal and technical verification, so security is one of the major priority while handling many systems at one time. Proposed solution of implementing the cryptographic techniques in Legal and Technical Verification into the existing Finnone System would help bank to overcome challenges of secure integration and connectivity issues at both ends.

***Recommendations:***

* Since the company has a lot of cash reserves and surplus with good amount of cash flow, company should invest more towards security and implementing cryptographic techniques in each and every system and hence boost the weaker areas in organization itself to make them healthy units.
* Bank can also think towards acquiring small and sick units to enhance the functional capabilities and help them generate more revenue with customer satisfaction.
* Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique.
* DES is now considered to be insecure for some applications like banking system. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable.
* DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

1. **FUTURE SCOPE**
   * An increasing demand for a digital banking experience from millennials and Gen Zers is transforming how the entire banking industry operates.  As more and more customers are now approaching for Home Loans, more number of people are increasing day by day, so banks are disbursing more loans to people.

With this, fraud are also increasing at a higher rate, hence more and more secure cryptographic techniques are required and therefore scope is at a broader level in future.

* + Consumers' growing desire to access financial services from digital channels has led to a surge in new banking technologies that are reconceptualizing the banking industry.
  + In addition to the future of banking coverage, Insider Intelligence publishes thousands of research reports, charts, and forecasts on the Banking industry.
  + Digitalization is changing how people interact and do business on a day-to-day basis, and advancements in banking technology are continuing to influence the future of financial services around the world. An increasing demand for a digital banking experience from millennials and Gen Zers is transforming how the entire banking industry operates.
  + From retail and mobile banking, to neobank startups, technology has its hand in seemingly every aspect of the banking industry; and, the influence of technology will continue to launch banking into a digitized future.
  + Retail banking, also known as consumer banking, refers to the specific services banks can offer to consumers–such as savings and checking accounts, credit and debit cards, and loans. Consumers' growing desire to access financial services from digital channels has led to a surge in new banking technologies that are reconceptualizing the entire retail banking market.

## *Future of Retail Banking*

## Technology geared toward improving retail banks' operational efficiency is positively impacting the market. According to Insider Intelligence, 39% of retail banking executives say that reducing costs is where technology has the greatest impact, compared to only 24% who say  it's improving customer experience.

## Retail banks are also launching platforms in the[Banking-as-a-Service (BaaS) space](https://www.businessinsider.com/banking-as-a-service-industry) to remain competitive. For example, UK neobank Starling used to exclusively offer business-to-consumer (B2C) retail banking services; but, after launching a[BaaS platform](https://www.businessinsider.com/banking-as-a-service-platform-providers), Starling diversified its product and revenue streams, helping it remain relevant in the neobank space.

## Meanwhile, mobile banking has solidified its place as a must-have feature for financial institutions to remain competitive, particularly among digitally-savvy millennials and Gen Zers. In fact, over 45% of respondents to Insider Intelligence's fourth annual [Mobile Banking Competitive Edge Study](https://www.businessinsider.com/us-mobile-banking-competitive-edge-study-2020) identify mobile as a top-three factor that determines their choice of FI.

## *Future of Mobile Banking*

## Mobile banking has become the go-to method for users to make deposits, account transfers, and monitor their spendings and earnings—and a key differentiator for banking leaders. Nearly 80% of our survey respondents who have used mobile banking say it is the primary way they access their bank account.

## Since the onset of the coronavirus pandemic, mobile capabilities is a more significant factor in bank selection among respondents than it was last year. Financial institutions should understand which mobile banking features consumers value most and where they stand compared to their competitors, so they can pinpoint specific areas to devote the most attention to.

## The foremost concern consumers have when mobile banking remains security. The fear of data breach increases the demand for services that keep users' data secure–allowing consumers to place holds on credit or debit cards, schedule travel alerts, and file and review card transaction disputes are some successful security banking features.

## Online banking, which includes mobile banking, refers to the overall experience of banking through digital channels, including mobile apps, desktop, live chatbots, and more.

## *Future of Online Banking*

## The popularity of mobile banking has surpassed that of online banking, and the overall number of online customers has slowed worldwide. According to Insider Intelligence, mobile banking is growing at five times the rate of online banking, and half of all online customers are also mobile banking users.

* Despite this growing popularity, some banks still fall short on the demand for mobile tasks, like bill pay and reward redemption, causing them to push users to online banking. However, even this push won't be enough to popularize online banking as millenials and Gen Zers continue gravitating toward the mobile market.
* Digital-only banks, also known as neobanks, are redefining the future of banking around the world. Though off to a slow start in the US due to high regulatory barriers, recent developments and the loosening of regulations suggest that US neobanks are set to take off.

## *Future of Digital-Only Banks*

* Sophisticated mobile banking tools are a top factor fueling US neobanks' stratospheric rise—one that's taken on more importance amid COVID-19. Incumbent financial institutions, neobanks, and tech companies alike can benefit from understanding exactly how leading neobanks are raising the bar for customer expectations and trust to successfully scale their businesses.
* San Francisco-based Chime, the largest US neobank, has attracted over 7.4 million account holders by 2019, and is projected to grow this figure to 19.8 million in 2024. The development of more neobanks in the US will bring awareness to digital-only banking, and eventually wane-out traditional banking firms.

## *Banking Technology Trends*

* The future of banking technology is driven by consumers, especially Gen Zers, who see technology as something that enhances their lives. A common trend in banking technology is using an application programming interface (API) to make proprietary data available to anyone who has the consumer's permission to access it.
* APIs could be used to enable a bank's mobile app to pull down customer account information. Fintechs have also used API technology to enable their businesses to work, and their success is encouraging competitors to develop their own APIs.
* Additionally, Insider Intelligence reported that 48% of banking executives believe new technologies like blockchain and artificial intelligence (AI) will have the greatest impact on banking through 2020. According to Insider Intelligence, banks are exploring blockchain technology in hopes of streamlining processes and cutting costs.
* Consumers can already see AI being used by most banks through chatbots in the front office. Banks are using AI to smooth customer identification and authentication, while also mimicking live employees through chatbots and voice assistants.

1. **QUESTIONAIRE**

* Manual form were giving to HDFC Mortgage loan team.
* Survey was conducted online where different questions were presented about cryptography ciphers, RSA etc.

1. **BIBLIOGRAPHY**

* Books, Banks Forums, Economics Times, Outlook Money
* <https://www.hdfc.com/>
* <https://www.hdfcsec.com/>
* <https://economictimes.indiatimes.com/topic/HDFC-Securities>
* <https://www.hdfcbank.com/personal/resources/learning-centre/secure/safe-online-banking-tips-measures>
* <http://iosrjournals.org/iosr-jbm/papers/Conf.17037-2017/Volume-2/6.%2033-37.pdf>
* <https://www.essaysauce.com/information-technology-essays/essay-cryptography-security-in-the-banking-sector/>
* Common Cryptographic Architecture: Cryptographic Application Programming Interface
* Reference, SC40-1675, IBM Corporation (1992)
* W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on
* Information Theory IT-22, No. 6, 644-645 (November 1976)
* C. S. Kline and G. J. Popek, "Public Key vs. Conventional Key Encryption," American
* Federation Information Processing Societies Conference Proceedings, 1979
* A public key extension to the Common Cryptographic Architecture, Le, An V, Matyas,
* Stephen M, Johnson, Donald B, John D, Wilkins, IBM Systems Journal, 1993