# **ABSTRACT**

The increasing digitization of the banking sector has brought about significant advancements in customer service and transaction efficiency. However, this evolution has also introduced a range of security challenges, particularly concerning data privacy, transaction integrity, and vulnerability to cyber threats. Traditional e-banking systems, though efficient, are often susceptible to security risks such as phishing, malware attacks, and data breaches, which can compromise sensitive financial information and undermine customer trust. In response to these challenges, blockchain technology has emerged as a revolutionary solution that provides enhanced security, transparency, and decentralization, making it highly suitable for secure banking applications.

This project, **Secure Banking Using Blockchain**, aims to explore the potential of blockchain technology in mitigating the security risks associated with online banking systems. By leveraging blockchain’s decentralized architecture, cryptographic principles, and consensus mechanisms, this research seeks to provide a more secure and transparent banking environment. The study begins by reviewing the current state of traditional e-banking systems, identifying their vulnerabilities, and analyzing the security methods currently implemented by banks. Surveys and archival data are utilized to understand customer and banker perspectives on adopting blockchain-based solutions, with security emerging as the core concern for both groups.

The research further explores various categories of threats specific to both traditional and blockchain banking systems, such as **phishing, hacking, Distributed Denial of Service (DDoS) attacks, smart contract vulnerabilities, and 51% attacks**. A comparative study of existing security protocols in traditional systems (e.g., SSL, HTTPS) and blockchain mechanisms (e.g., encryption, digital signatures, consensus algorithms like Proof of Work and Proof of Stake) is conducted. The focus is on how blockchain’s **immutable ledger, decentralized control, and cryptographic methods** offer significant advantages in mitigating these threats.

Two blockchain-based encryption algorithms are presented as part of the project. The first algorithm, **NPN (Prime Numbers and Pseudo-Random Number Generator)**, combines cryptographic techniques to enhance the security of banking transactions by ensuring unpredictability and randomness in encryption keys. The second algorithm, **LIE architecture**, leverages a **multi-round encryption process** based on the **Fiestel network**, utilizing a set of **discrete cryptographic sub-keys and permutation matrices** to provide robust data security. The LIE algorithm also applies the blockchain principles of **confusion and diffusion** to maximize the difficulty of data manipulation and enhance transaction integrity.

Additionally, the research highlights the mathematical underpinnings of these algorithms, such as **XOR operations, multiplication**, and cryptographic hashing, which are critical to achieving essential properties like **avalanche effects, statistical independence, and completeness**. Both algorithms are designed to meet the stringent security demands of modern banking systems, ensuring that sensitive data remains secure during transactions.

To validate the performance and effectiveness of the proposed algorithms, a comparative analysis is conducted with existing blockchain encryption methods. The time and space complexity of the designed algorithms are optimized and evaluated to ensure they are both efficient and scalable for real-world banking applications.

The project concludes with recommendations for implementing blockchain-based security in modern banking systems, focusing on preventive measures to protect data from hacking, corruption, or unauthorized alteration. By proposing innovative cryptographic algorithms and optimizing their performance, this project contributes to the growing body of research on blockchain security in the financial sector and provides a practical framework for enhancing the security of online banking transactions.

**CHAPTER 1**

**INTRODUCTION**

**BACKGROUND OF RESEARCH**

Bank has been originated from Banco, which is an Italian word which means bench (all transactions were conducted while sitting on the bench) (yousigma.com). Originally, the Jews and later the goldsmiths were involved in money lending. Banks being financial organization were initially involved in depositing and lending of money. Banks now offer various facilities like accepting deposits, lending loans, credit/ debit card, foreign exchange, locker facility, paying bills and dues, ACH (Automated Clearing House), ECS (Electronic Clearance Service), etc. Banks are growing tremendously in terms of making cashless or digital transactions. Individuals, business house, corporates, etc. transact with banks.

Human always had the zeal to progress & improve the existing technologies. Technology has led to great development and growth, which has given a platform for further developments. Earlier, Traditional Bank had a physical branch (brick and mortar model), where the customers can directly visit and meet bank staff in person. Later, the facility of inquiring about the account information was handled via phone also popularly known as Phone Banking. Gradually ATMs (Automated Teller Machines) were introduced which made the life of bankers and customers very convenient. Customers can draw money anytime without worrying about the branch timings, and holidays of a bank by using ATM. With the innovation in information technology the development and availability of resources like internet speed has helped the customers to use the banking services 24\*7 anywhere, anytime with a lot of ease.

The Internet is one of the great advancement accomplished by humankind till date. The Internet has influenced different aspects of society. Through internet; the user can view stock market details, news, sports, and results of an examination, & can also access bank account, shop, communicate etc. Banking domain is extensively using and growing with the internet; they are offering various financial services online. The Internet offers significant benefits to society but also leaves various loopholes for severe crime. Dealing with the finances and customer-centric data; banking industry has turned into databank of sensitive information. Especially now, when customers are paying electronically through e-banking or any third party website, the banks needs security for the customers’ data and the transactions. The banks have successfully implemented E-Commerce (Kardaras and Papathanassiou, 2001). In India, after

demonetisation, the government is promoting digital India campaign. The banks & business houses are advised to keep modes of e-payments may be by APPs or POS machines or third party payment options.

Internet banking denotes the services offered remotely via bank on their website or now a days mobile apps (Suganthi, 2001; Dannenerg and Kellner, 1998; Zineldin, 1995). It is the fastest, easiest and efficient way of banking compared to traditional methods. Technology has instigated as a tactical resource for banks in attaining higher competence, managing the processes, increasing the efficiency & profitability. For customers, the ease & speed to access their bank 24\*7 all through the year and from any location is a very lucrative option. To sustain in the world of digitization, all industry including banks have been prompt to accept & use the technology in the best ways. Internet banking services are critical to handle customer demands, to enhance customer relationship management, face competition, and ensure better security. Banks requires relatively very less investment for e-banking as compared to traditional branch banking (brick & mortar model) (Burnham, 1996).

Services offered Online by banks- banking is maturing with time, initially the banks website used to be only informative, later the customers’ were given login credentials to check the balance and transaction history online, now various services like paying bills online, transfer money across different accounts, apply for loan online, shop online via credit/debit/net banking, etc. are available. Banks are launching the Mobile Apps with enhanced features like biometric for making online transactions more secure.

**Benefits of Online Banking-**

•Ease/ Convenience- Internet banking have made the life of clients and bankers very easy and comfortable. Customers may not visit the bank often for every small thing like getting the passbook updated; know their account balance, money transfer, paying bills, etc.

•Timings are Flexible- Customers can transact online according to their convenience, no time constraints and no location issue. The customer can negotiate 24\*7; all 365 days.

•Speed- The total transaction time has been reduced. It has speeded the task and widens the distance.

•Green Environment- The focus is to keep the environment green & saving the trees; by not wasting papers in taking the printouts, updating the pass books, sending the letters for the non-payment or due amount for the credit card. The banks quickly accomplish this by sending emails and SMS (Short Message Service) for credit card payment, or non-payment of the loan amount or any additional communication. Customers get account balance message on every transaction. The customers don’t have to spend money on commuting which is again beneficial for the environment.

•Banks Reputation- Living in a competitive world, even the banks needs to handle the customers in the best way. Customer Satisfaction is a must for the banks & thus they are offering better CRM (Customer Relationship Management) techniques. The banks are upgrading themselves technologically to be capable to provide best facilities online. The banks need to revert to the customers’ queries within a stipulated time.

•Cost- Effective- E-banking is cost effective to both the customers and the bankers. Banks may not invest in opening more branches rather they can focus on opening more ATMS. They save by hiring fewer employees, consuming less electricity, fewer prints, and other facilities required in a traditional way, and customer saves time in commuting, calling, and standing in queues etc. “time is money”.

**Limitations of Online Banking-** Every coin have two sides. Similarly, internet banking also suffers from the following issues

•Security-Security is considered to be a matter of great concern to be worried for such attacks. Attacks like-phishing, hacking, cracking, net extortion, salami attack etc. are making the customer little more reluctant, hesitant to transact online.

•Laws- Laws for e-banking are in its adolescence age. E-banking has no national or state boundaries to monitor the crime. The crime is more severe and to punish the culprit the laws are very less.

•Other challenges- Naive customers, no personal communication and relation with banks, etc.

Online Transaction- The user can shop and pay digitally via plastic money, Digital Wallet, Electronic Cash like Mondex, E-Cheques etc. Electronic Payments system leaves the opportunity for a criminal to vigil every transaction and a possibility to even breach the information (as every transaction traverse via an open insecure channel). Therefore, the bank should be watchful for securing the information. The more severe phase of online transactions is confirming the safety of e-payment (E. M. Awad).

While transacting online, security remain a key element to worry for banks. Banks are aware that for attaining a high confidence and trust from both the business houses and customers, their information security has to be ensured. Therefore, the banks, other financial institutions, card associations, and vendors are developing an Internet payment infrastructure. Banks have adopted many security procedures like the virtual keyboard which protects from attacks like key loggers, OTP, Grid Matrix and 3D PIN for making transactions more secure to be hacked/ cracked by a hacker. It is recommended to use 2D or 3D authentication for privacy and security check.

While making an online transaction the users interact with merchant store, banking site or some third party payment gateway. The information can be breached at customers end, merchant store, bank or third party site if system is compromised. Maximum breaches take place while information is travelling from the customers end to the merchant/bank end. The moment user clicks submit button for making the transaction on either the merchant site, bank site or third party financial site like Paypal, the information can be breached easily as sent via internet (an insecure channel) (Sharma, 2014).

The Encryption algorithms are designed and implemented to safeguard the data from unethical hacking. Various protocols like SSL, HTTPS, and TLS etc. are used to ensure the security of the path from where the data will traverse. These protocols extensively used encryption algorithm for securing data. Like SSL, earlier uses DES algorithm for safety of data and now use AES algorithm with 128 bit keys for a secure path for exchanging information. HTTPS primary goal is to provide security on every transaction or transfer. HTTPS along with SSL complement each other as they doubly verify the security. The security is ensured for the path and simultaneously on every transaction per transfer. Encryption algorithms are used to login the bank site. When user inputs the password while login; the password gets converted from 6 digit number to a bigger number (64/128 digits) before travelling further. These days encryption is used everywhere even a mobile phone without an internet connection uses RC4 stream cipher encryption algorithm. Even various Mobile apps like Whatsapp use encryption technique for data protection.

Confidentiality of information is a necessity in this era, and cryptography is an indispensable tool for protecting data. It is the technique of writing a message in a strange form; a message which is incomprehensible, scrambled or meaningless from a naïve person’s eye. It is an ancient way of shielding the information from any intruder or unauthorized user. Cryptography provides access to only an authentic user who possesses the key. Encryption-Decryption are two processes which are beneficial in implementing cryptography. In case the data is being hacked by the hacker, the hacker is unable to read and retrieve the original message rather the opponent will get a cipher text which he needs to decrypt/decode. Cryptography for encrypting involves an encryption algorithm and a key to attain the cipher text from the given plain text. Decryption is the reverse of Encryption.

The cryptography techniques falls under two techniques one is Symmetric and the other is Asymmetric Key encryption algorithm. Symmetric Key signifies the use of one, single or unique key used for enciphering and deciphering the code. Key is shared prior to the communication of the message only with sender and receiver. Asymmetric Key deals with two or a pair or set of keys used discretely for sending (encrypting) and retrieving (decrypting) the message (Govinda, K., & Sathiyamoorth, E., 2011).

The thesis deals with the in depth study of symmetric key encryption algorithm. The existing algorithms were studied and analysed, followed by proposing and implementing two new symmetric key algorithms. Further the algorithms have been compared on various parameters of architecture, flexibility, security etc.

**MOTIVATION OF RESEARCH**

The literature was studied in pursuit of knowledge for electronic banking and security in the line of questions cited below.

➢ How are customers responding to the adoption of blockchain-based secure banking systems?

Analyze customer acceptance and trust in blockchain technology for enhanced security in banking transactions.

➢ What critical information is stored or processed by banks using blockchain?

Highlight the types of sensitive data such as customer identity, transaction details, and financial records managed securely through blockchain.

➢ What are the potential security threats to this critical information in blockchain-based banking?

Discuss specific threats such as hacking, data breaches, or smart contract vulnerabilities that could compromise banking information.

➢ How do these security threats impact banks and their customers?

Explore the consequences of security breaches, including financial losses, loss of trust, and legal implications for banks and their base customers.

➢ How is information communicated within the bank and across the blockchain network?

Explain the decentralized nature of blockchain, peer-to-peer communication, and how data is securely transmitted between bank nodes.

➢ How is sensitive information protected when shared on public blockchain networks or during private transactions?

Detail the role of encryption, hashing, and secure consensus mechanisms that safeguard data both in public blockchains and private banking transactions.

➢ How can blockchain’s encryption algorithms further secure online transactions?

Highlight the use of cryptographic techniques like asymmetric encryption, digital signatures, and smart contracts to ensure secure and tamper-proof transactions.

Going deep into ways of protecting most critical information, it was observed that encryption algorithms play a significant role. Hence security is the core aim with the specific objective to analyse existing algorithm & design a new algorithm for achieving/attaining the same goal. Therefore, an extensive review was done in context to encryption algorithm especially Symmetric Key: block cipher, and stream cipher.

**NEED FOR RESEARCH**

Development in technology has led to paradigm shift from conventional (traditional) banking (brick and mortar model- Physical branch) to online banking. As banks deal with financial information and customers’ demography (personal information), a need arises to study electronic banking to consider the criticalities of e-banking. The key issue being Security; is continuously an interesting area of research.

For all the parties conducting online transactions, security is of utmost concerns. Numerous methods have been designed and implemented for improving the security around online transactions. But then there remains a scope for improvisation as cybercrimes and threats are anonymous, and they cultivate with the growth of the technology. The crimes and threats being unknown are tough to test and validate. The banking sector has grown and taken significant steps to safeguard the customers via OTP, Virtual Keyboard, 3D Pin, Grid Matrix, etc. (Sharma, 2015). Banks are using secure path via SSL, TLS, HTTPS, etc. Encryption algorithm provides security from any intruder/ hacker; still, there exits scenarios of hacking which shows a need of improvisation. The thesis aims to build a secure symmetric key encryption algorithm for enhancing safety of user data while transacting online.

**RESEARCH OBJECTIVES**

➢ Explore the Blockchain-Based Banking Sector and the Security Issues They Face.

Examine how blockchain technology is applied in secure banking systems and the key security challenges banks encounter.

➢ Analyze the Impact of Blockchain Security on End Users in Banking.

Investigate how blockchain’s enhanced security features influence the user experience, trust, and overall adoption of secure banking solutions.

➢ Anticipate Potential Security Threats That Could Compromise Blockchain-Based Banking Information.

Identify possible security threats such as 51% attacks, private key theft, or vulnerabilities in smart contracts that may affect blockchain security.

➢ Conduct a Comparative Study of Existing Blockchain Algorithms for Securing Online Transactions.

Analyze and compare algorithms like SHA-256, elliptic curve cryptography (ECC), and consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) in securing blockchain transactions.

➢ Design a Blockchain-Based Algorithm to Ensure Secure Online Transactions.

Propose and design a secure blockchain algorithm aimed at enhancing transaction safety, data integrity, and privacy in banking.

➢ Compare My Blockchain Algorithm With Existing Algorithms.

Evaluate your designed algorithm’s performance in terms of security, efficiency, and scalability against widely used blockchain algorithms.

➢ Suggest Preventive Measures to Protect Blockchain Data From Being Corrupted, Hacked, or Altered.

Propose strategies such as multi-signature authentication, improved consensus mechanisms, or enhanced encryption methods to safeguard data on the blockchain.

➢ Optimize the Algorithm and Verify Its Time and Space Complexity Compared to Existing Blockchain Algorithms.

Assess the efficiency of your algorithm by measuring its computational time and space complexity, and compare it with other blockchain security algorithms.

SCOPE OF RESEARCH

S The study begins by reviewing the archival data on customer behavior towards the adoption of blockchain in banking systems across various regions, the vulnerabilities present in current centralized banking systems, and solutions already implemented by banks using blockchain technology. This was followed by analyzing surveys conducted with both bankers and customers. The study found that security remains the primary reason for users' hesitation in adopting blockchain-based secure banking. Additionally, the research explored various categories of threats such as smart contract vulnerabilities, 51% attacks, private key theft, and double-spending. Several blockchain security methods such as encryption, digital signatures, and consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) were examined. The focus was placed on decentralized encryption and cryptographic techniques which ensure data safety and integrity within blockchain networks.

The thesis demonstrates two blockchain-based encryption algorithms. The first, NPN, uses a combination of Prime Numbers and Pseudo-Random Number Generators (PRNG) to enhance security. The second algorithm, LIE architecture, follows a smart contract-based framework with multi-round encryption, leveraging discrete sets of cryptographic keys and hash functions to secure data. LIE also employs the fundamental blockchain principles of confusion and diffusion, ensuring high resistance to attacks. Both algorithms use core mathematical operations like multiplication, XOR, and hashing to achieve key properties critical to blockchain systems, such as immutability, decentralization, and high fault tolerance.

# **CHAPTER 2**

# **Literature review**

Literature was examined in the quest for the knowledge of security in e-banking. Review begins by seeing the adoption pattern; followed by analyzes of the adoption trend. The researcher was curious to discover the dangers and crime which can breach the security of online banking. Later the research moved to various securities methods adopted by banks like applying anti-virus, firewalls, using SSL, HTTPS, OTP, Grid Matrix, virtual keyboard, anti-phishing, and biometric, etc. Gradually the focus was shifted on securing the online transaction especially after the payment is made. Paying online is a serious concern as the credentials might go in some wrong hands. Consequently here is a need for ensuring security by restricting the hacker to recover the original data. Finally, an extensive literature has been studied on cryptography, especially Symmetric ciphers like Data Encryption Standard, AES, 3DES, Blowfish, etc. and several Asymmetric algorithms like RSA, ECC, etc.

Online Banking

Adoption of IB

Security Threats

Security Measures

Hacking/ Cracking

Biometric

Anti-Phishing

Anti-Virus

Cryptography

Others like SSL, HTTPS

Phishing

Symmetric Key

Asymmetric Key

DDOS

DES

RSA

Key Loggers/ Malwares

3DES

ECC

Salami Attack

AES

BlowFish

IDEA

Fig. 2.1 Study of Review

* 1. **ONLINE BANKING**

Banks clamps a major role in global economy. Technology has foreseen the innovative thinking and conducting business. Technology especially internet and smart phones have proliferated the opportunities for banks. Technological changes have a tremendous result on the organizations; even the approach of performing tasks, interacting with customers (better CRM) and, conducting their business has become much speedier and easier (Freeman, 1996; Crane, 1996; Jayawardhena, & Foley, 2000). Technology has also transformed the way monetary facilities are planned and provided (Liao, 1999; Schneider, 2006; Ozdemir, 2008). Electronic banking (e-banking) is the current interactive communication channel offering bank products and services straight to the bank clients electronically (Daniel, 1999; Sathye, 1999). James

H. Clark, co-founder and chairperson, Netscape Communications, firmly believed that besides telephones; the best thing that has happened due to telecommunications is the Internet. He also had a vision that internet will be essential for the growth of any business. No business will sustain without an Internet connection, as telephone is an elementary part of any organization (Clark, 1996). (Grandy, 1995) The first virtual bank namely “Security First Network Bank” was inaugurated by USA in October 1995. This bank does not have any physical branch (virtual bank is based on the concept of a non-branch bank), as the user can transact without actually going to the bank. It gives the provision to the banks to connect virtually via ATM, Telephone, PCs and Internet (Tan & Teo, 2000; Aladwani, 2001).

# Factors influencing the E-banking

Banks had envisioned that online banking will not complement but replace the conventional form of banking (Soh, 1997; Jayawardhena, & Foley, 2000). Adoption is a technique of accepting and continuing the habit of a particular idea or service. (Gerrard, et al., 2006) Various models are used as a powerful framework for predicting Technology Acceptance Behavior (Szajna, 1994; Igbaria, 1995; Gefen, 2000; Chau, 2001). There are various prototypes like Theory of Reasoned Action, (Ajzen and Fishbein, 1980), Theory of Planned Behaviour (Ajzen, 1985); Technology Acceptance Model, (Davis, 1986; Davis et al., 1989), etc. Technology Acceptance Model was (Wang, et al., 2003; Jaruwachirathanakul, & Fink, 2005; Nasri, & Charfeddine, 2012; Kabeer, 2013; Kurnia, 2010) most influenced models because of the (Adams, 1992) factors like perceived usefulness, ease of use and credibility (security & privacy).

In (Chau, 1996; Sathye, 1999) their researches have highlighted factors which are key factors for adopting online banking. Conferring the study (Howard and Moore, 1982; Cooper, 1997; Daniel, 1999; Sathye, 1999; Goudarzi, 2013), Customer awareness is a must. If the client is unaware of the facility and its benefits, will never adopt it. Internet banking could be opted only with customer’s attitude, willingness and satisfaction (Hanafizadeh, P. et al., 2013). The study added the descriptive, related and comparative

literature for adoption, along with customer segmentation, satisfaction & loyalty. Second factor important in influencing adoption is the ease or user friendliness to use and understand (Daniel, 1999; Rogers, 1962; Cooper, 1997, Wall, 1997). Users will be comfortable if even a naïve user can understand and operate. The third factor is the risk involved. Internet security has been considered as the utmost important challenge for online banking (Gandy, 1995; Wills, 1996; Tan, 1996; Cooper, 1997; O’Connell, 1996; Daniel, 1999; Hoffman et al., 1999; Aladwani, 2001; Perkins, 2013). Online banking safety range has widened from securing just the personal information to actually securing the financial loss (Sayar and Wolfe, 2007). The fourth factor is the price/cost. It should be reasonably priced else adoption will be difficult (Wallis Report, 1997; Cooper, 1997). The fifth factor was a particular need to move from existing brick and mortar (traditional branches) to new technology. Finally, the availability of resources (infrastructure) is most significant in influencing the growth of adoption (Akinci et al., 2004).

Research depicts retail banking services, distribution channels, consumers’ attitude and banks’ perception as interconnected areas for smooth running of the banks. The banks offered financial services through various channels like phone banking, internet banking, home banking, etc. This is shared and shown to the consumer to analyze customer’s behavior and readiness for accepting e-banking. Last but not the least banks’ perception and approach towards internet banking plays a pivotal role to gather the bank’s perspective for the obstacles or barriers in adoption, strategic value in implementation etc. As reported in a study conducted in Pakistan (Shaikh, 2014; Maitlo, G.M., 2014); has found five significant factors i.e. channel convenience, Risk, security, awareness about internet, and knowledge on online banking which have persuaded the acceptance towards online banking. (Jayawardhena, & Foley, 2000) has highlighted the challenges that lie ahead for banks are customer satisfaction as the needs are complex and challenging to manage, an improved competition not only from within the sector, but also from new entrants entering into this field. The third essential point focus on the demands placed upon on the supply chain. Lastly, the products and services needs to be developed and upgraded persistently according to the desired change (Jayawardhena, & Foley, 2000).

# Delivery Channels and Banking Services

E-banking has gained popularity in recent past. On-line banking has come as a solution to countless shortcomings of conventional branch banking. Initially, e-banking has initiated as just another way or platform for interacting with the bank clients. (Shani, 1992) study depicts e-banking has made it convenient for bankers to aim customers with greater precision than earlier and build a better relation by guiding and helping them. Primarily there are four channels to bank, i.e. physical branch, ATM, Phone banking, and internet banking. (Kass, 1994; Mitchell, 1995) Findings indicate, ATM as the most preferred

way to transact; trailed by online banking followed by branch banking, and lastly telephone banking. (Makris et al., 2009; Sathye, 1999) E-banking is the easiest and modern way to offer retail banking services. Internet banking provides an opportunity to transact online from anywhere, anytime in a cost- effective and efficient way. Initially, the bank websites were informative; which means site discuss general information about the products and services offered (Sathye, 1999; Mishra, n.d; Syamsuddin, & Hwang, 2009). Various services were introduced later by banks such as retrieving account details, fund transfer, and purchasing financial products like Life Insurance, Shares etc. Online services like buying goods or services, paying bills etc. gave the user the permission to clear their dues using bank’s website called “transactional” online banking (Dannenberg and Kellner, 1998; Shaoyi,. et al., 1999; Wan, 2004). (Hagel and Hewlin, 1997; Howcroft et al., 2002) Banks prefer multi-channel banking services rather than relying upon any single method. According to (Kayode, 2008) the study depicts various bank services offered to a customer online like fund transfer, transactions with different banks clients and accessing their accounts details along with the balance. One of the significant tasks is to cope up with the service quality. Service quality depends on customer beliefs of the service, organization reputation & image, aspect of service setting; real service encounter and customer participation (Gronroos, 1984; Parasuraman et al., 1985, 1991; Broderick, 2002).

# Drivers to encourage Customers and Bankers

Consumers and banks are both getting the benefit of using online banking system (Jayawardhena, & Foley, 2000; Howcraft et al., 2002; Liao, 2002; Akinci, 2004; Albadvi, & Gharaee, 2009; Sharma, & Garg, 2012). There are various options as given below which motivate the customers to go for Internet banking:-

* Providing faster and easier service to customers,
* Reducing operational cost (paperless environment, geographical convenience, no travelling cost and standing in queues (Chan,2001),
* Reducing workforce (fewer branches and less staff),
* Creating new market,
* Improving bank’s image (better customer satisfaction),
* Time efficiency (24\*7),
* Good service quality (Transfer of Funds, Asset Management, Loan application, etc.),
* User-friendliness,
* Accuracy,
* User experience,
* convenience,
* The reliability of bank and privacy.

# Bankers’ Perspective

(Jayawardhena and Foley, 2000) The major advantage of using online banking over traditional banking is saving the cost, getting new sections of the populace, proficiency, improvement of bank’s reputation and better service with improved CRM. Enhanced branding and improved responsiveness to the marketplace are one of the greatest benefits (Nami, 2009). While comparing e-banking with traditional banking; Electronic banking has not only reduced the cost but has also provided better customer satisfaction as banks have complete and updated customer information and better service quality (Gerrard, 2003; Rouibah et al., 2009; Sharma, 2012). The study illustrates that (Pikkarainen, 2004) cost reduction and reduced traditional (physical) branches were considered as two key factors for the rapid growth of e- banking. Lower costs in comparison with traditional branch banking are possible because of reduced branches which has immensely cut down the cost (staff cost, office space overhead, physical branch expense, printing and mailing cost, etc.). The study analyzed by (Sohail, 2008) portrays that bank managers know and understand customers’ perception for online banking service quality. Subsequently the bankers have to focus on improving customer satisfaction with the online aspects of service quality. Three factors which, influence users’ Service quality are “efficiency and security,” “fulfillment” and “responsiveness.”

# Customer’s Perspective

Internet banking seems more useful than any other channel offered by bank. According to (Rogers and Shoemaker, 1971) consumer accepts or rejects innovation when the customer becomes aware of the product. New ideas and innovations have turned as a biggest disaster in the market majorly because of customer dissatisfaction and resistance. Therefore, it is essential for bankers to know and inquire about the customers’ behavior; as in how customers feel about this technology (Lassar et. al., 2000). (Laukkanen, 2007) Online banking has permitted almost all transactions at a single mouse click, except money withdrawal throughout a day. Bank clients with logic, awareness, and accessibility are upgrading to the new channel. They prefer "internet banking" over branch banking as branch banking make the customer wait in queues, has a time restriction (Kerem, 2008). Thus customer prefers e-banking because of its convenience. The greatest advantage is it’s inexpensive or even free to clients. The research findings (Mashhadi, 2007) shows that three out of four customers are keen to access e-banking. Customers are using online banking to speed up the task by investing less time and also because of the convenience, user-friendliness, accessible anytime, can be easily tracked and reduce the cost (Baldock 1997; Kerem, 2003). They are looking for more lucrative options in multiple areas (Devlin, 1995).

# Geographically dispersed customers’ adoption behavior for e-bankingg Regardless of all the advantages for customers, adoption rates vary across countries. According to (Tan and Teo, 2000) consumers’ attitude, behavior, and social influence are few factors which led to adoption. As per (Akinci et al., 2004), research was conducted to understand the behavior of customers, two groups were formed based on demographic profiles, attitudinal properties and preferences for service delivery channels and were called Adopters/ Users or Non-Adopters/ Non-Users (Gerrard and Cunningham, 2003). As per (Kurnia, 2010) a study conducted on Chinese; identified security as a root cause because of which the customers are hesitant for online banking. (Gerrard, 2006) concluded the paper by identifying two frequently mentioned factors which are restraining the customers from using online banking were risks and the lack of perceived need. The study (Jaruwachirathanakul, 2005) illustrates “Features of the website” and “Perceived Usefulness” as the influencing elements in e-banking adoption by Thailand users. In the study conducted by (Jayawardhena, 2000) has observed that the banks are even functioning in a very competitive environment. Therefore, there is a need to please the customers demand and give them best service and financial benefits (low interest rate, high FD rate etc.) to retain them. Banks have to address the demands placed on the supply chain. Finally, it is essential for banks to constantly upgrade products and services. (Aladwani, 2001) The study conducted on eight banks of Kuwait found Internet security as a major challenge for acceptability. Trust was another significant factor which has impacted the acceptance of e-banking (Suh, & Han, 2002; Goudarzi, 2013). Customer perception of security can be increased first by making online transactions more convenient and useful, second by assuring clients and last by offering customers a personalized experience (Singh, 2006; Perkins, 2013). A study (Ndubisi, & Sinti, 2006) on Malaysian customers depicts that the features offered by banks on their website and customer’s belief helps in following e-banking. The study (Malhotra, & Singh, 2007) is based on the number of banks which offers Internet banking; a rare variable. From the results it is observable that the larger banks, recently opened banks, privately owned banks, banks with higher expenses for fixed assets, banks with higher deposits and lower branch intensity are going for new technology. Perceived risk and interpersonal influence are the two critical factors. The study (Albadvi, & Gharaee, 2009) illustrates Karafarin banks the problems like ICT infrastructure and political issues faced by them. (Sathye, 1999) Results justify the slow acceptance of e-banking in Australia is due to the lack of consciousness and security. Demography also has been observed as a main reason to opt for e-banking. (Al-Ashban, 2001; Karjaluoto, 2002; Sathye, 1999) Nine factors were identified as an obstacle in following e-banking. They are cost, reliability, processing barriers, security issues, technological inconsistence, lack of infrastructure, conventional approach, risk and resistance (Peterson, et al., 2011; Singh, 2013). (Mattila, 2003) research highlights that household earnings; qualification and learning effects the approval of Internet as a banking channel. A research conducted in Hong Kong, to identify the important reasons for Internet Banking Adoption has given transacting online from anywhere, anytime and reduction in processing time as the

top features to accept e-banking (Yiu, 2007). (Robinson, 2009) research depicts that a relatively modest population of Caribbean customers are using e-banking because of high level of awareness of e-banking services. They are accessing internet banking for checking balances and paying bills. The population has a high degree of insecurity which restricts them to go for e-banking. According to a study (Preeti, 2013) conducted on semi-urban areas; to know and observe the customers’ perception to avail the facility or not. From the study it was analyzed that to enhance the acceptability in semi-urban areas it is essential for a customer to know computers and have a hands-on the Internet.

The research (Sayar, 2007) portrays the primary difference in banks’ approach to deal with security problems in different countries. Online banking offers many services to the customers at anytime, anywhere like check balance, fund transfer, bills payment etc., via a telecommunication network. Developing country like Turkey offers a wider range of services and they completely rely on the technology to avoid fraud. On the contrary, a developed nation like UK with better infrastructure and a better environment feels reluctant to offer more services as they use conventional method to handle security (Sayar, 2007). In a different research carried by Dr. Clare along with his friend researched in the year 2012, focused on comparing Jamaica and UK on e-banking and e-fraud. Although Jamaica and the UK primarily begin with the similar commonwealth platform; disturbed by the credit crisis and had to control and monitor e-banking and the e-fraud that has arisen. But the UK has plenty of regulations and policies and more instruments to tackle cyber-crime. (Govender, 2013) South Africa, as an emerging nation has a well-developed infrastructure, a decent consumer base with sufficient purchasing power, but a low penetration rate.

E-banking has identified competitive edge, and service quality as significant feature to remain in the business. Service quality, a prime factor in the adoption; directly related to customer satisfaction. Geographically wide work and researches have been carried out. The researchers have designed different models like SERVQUAL (Service Quality), SERVPERF (Service Performance) (Cronin & Taylor, 1992). Dimensions like site aesthetic and customization for a bank website are also considered important factors when it comes to adoptability (Zavareh, 2012).

# Issues in Internet banking

E-banking is useful and fastest growing activity online which keeps a track of the finances. It is very smooth, speedy, and has given the flexibility to the users to transact and pay their utility payments worldwide. Universally it has enhanced the businesses of the organizations (Singh, 2007). (Martino, 2008) observed that there is no specific level of security, no well-known standard that banks need to consider while making the bank website, but there are some sets of guidelines for the same. For instance- PCI

(Payment Card Industry), DSS (Data Security Standard) and VISA agreed of complete requirements for safeguarding the payment.

There are few issues which can be regarded as a hurdle for online banking (Sathye, 1999; Gerrard, 2003; Polatoglu, 2001; Rotchanakitumnuai, 2003; Nami, 2009; Sharma, 2012). According to (Douglas and Loader, 2000) any illegal or illicit activity like illegally transferring money (Wall, 2001) from someone else’s account facilitated via computer on global networks is a severe security breach. (Hole, 2006) did an extensive research in Norway and reported several key security issues and has depicted how bank security is vulnerable for potential attacks.

After various researches few factors like trust, Authentication, Non-Repudiation, Privacy, Availability and Security has impacted the practice of online banking. (Claessens, 2003; Lampson, 2004; Stallings, 2011) As shown in fig. 2.2, CIA triad has three security objectives like- Confidentiality, availability, and integrity. Accountability and Authenticity also show an essential role in attaining security.

Confidentiality

Data &

Services

Availability

Integrity

Fig. 2.2: The Security Requirement Triad (Stallings, 2011)

After exploring various studies and surveys; security, has been identified as a critical issue which comes as a difficulty and makes customers bit hesitant and reluctant to transact and shop online and is a serious matter from the business perspective too (Ernst& Young, 1999). Safety of information is always valuable to the organizations. Safety is a must; especially when dealing with e-banking as financial transactions are involved. Online Banking has allured the hackers/ crackers/ criminals, and has been a great source for generating major revenue for offenders. Banks & Companies like MasterCard fear customers to transmit

their credit card details online as they are prone to security attack by some hacker (Info World, 1993; The Straits Time, 1995).

* 1. **SECURITY THREATS**

Security is a danger, which can cause damage to the resources by altering the data or disclosing the information, by wasting the resources by denial of service, and fraud (Kalakota, 1997). In context to safety there are few important terms like Vulnerability, Threat, and Attack (Whitman, 2015; Gregory, n.a). Vulnerability signifies flaw or fault in the built or design, configuration which might lead to exposure (attack) or is susceptible to a risk. Threat characterizes a continuous risk to an asset; it can interrupt the process, working, reliability, or accessibility of a network. Threat is intentional or unintentional and it has the possibility to cause damage. Whereas, Attack is done intentionally with an aim to cause damage or make losses.

Banks need to be extra cautious as the customer personal information along with the financial details is at stake. Hackers are not just attacking the bank but are also attacking the individual customer and are taking away the necessary details like credit card/ debit card credentials etc. (Stallings, 2011). There are numerous threats (Sharma, M. & Garg, R,B, 2012; Sharma, M., & Dwivedi, S., 2013) which are bothering the internet users like hacking, cracking, salami attack, phishing, malware, net extortion, spoofing, denial of service attack (DOS & DDOS), cyber stalking, defamation, IRC crime, etc. (Haneek, 2008). Bank customers faced the following threats/attacks-

***Phishing & Spoofing-*** Phishing & spoofing are both hacking attacks. (Nsouli, 2002) Phishing is a frequent attack meant to steal money illicitly from the bank (Roger, 2008). A phishing attack transpires via spam email or wrong domain name (URL). (Wada, 2012) These spam emails are usually sent in bulk (mass mailed). The targeted user is asked to click the link in which he needs to enter his credentials on a fake website, which will be spoofed later by the attackers. Spoof means to hoax, deceive, trick or imitate someone; which is easily accomplished once the user system is compromised or the user credentials are with the attacker.

Phishing can also occur by accessing a wrong URL. Suppose a hacker has designed a similar website as the bank website and has a similar URL or Domain name to confuse the naïve user (Matthew, 2008). Assume the bank customer by mistake typed [www.citibank.net](http://www.citibank.net/) as an alternative of Citibank.com or citybank.com (Chellappa, 2001). After clicking the wrong URL, the client will login his credentials and the moment he clicks submit; the details will be leaked. Later the user credentials will be spoofed or hacker will misuse/sell them. Phishing can be refrained or curbed by educating the customers

(Kumaraguru, 2007; Devarakonda, 2010), warning them not to share the password, check the link before sharing the credentials, using security toolbars (Sharif, 2006), etc. Earlier the bank used to send training materials through emails (Alnajim and Munro, 2009) but now specialized training on anti-phishing is scheduled for customers for better retention.

Phishing word has come from the word "fishing" (Aburrous, 2010). As a bite is thrown out with the hope to grab a fish similarly in phishing a mail or wrong URL is thrown to catch the user credentials. First phishing case was reported in 1996 Occurred at AOL (America Online). (Moore and Clayton) Year 2007, has estimated that around 350 million dollars and 311,449 people fall prey to phishing.

***Malicious Programs-*** The reason of spreading such programs (malware) is to encroach upon the confidentiality, integrity and authenticity (Singh, 2013). Malicious software is designed by the attacker after identifying the loopholes and weakness in the OS, designing, configuration etc. which makes the software prone for any cybercrime. As displayed in the below figure 2.3(Stallings, 2011) some software’s can be resident (independent replicating program- doesn’t require any host program) and non-resident software (requires host program for its functioning). **Virus**- Vital information resource under siege, name says it all; infects the computer and damage the resources like information, data speed etc. For example, downloading a game from the Internet would be dangerous because Malware in the form of Trojan or virus can affect the client software after it is on the local disk. Such games or infected files require software-based protections and hardware-based protections. For Example, Key Loggers is malicious software, which scans and logs keystrokes and sends these records to an attacker, one such incident was reported in 2012 at the South Carolina “Department of Revenue” (Alpna, 2016). Logic Bombs will activate on a specific date like 13th, Friday or a particular event.

Trap Doors

Non-

Resident

Logic

Bombs

Trojan Horse

Malicious

Programs

Viruses

worms

Resident

Zombie

Fig. 2.3: Classification of Malicious Programs (Stallings, 2011)

***Hacking/ Cracking*-** To crack or hack into other person computer and steal all important information. Unethical hacking has always remained a serious concern (Harmon, 1995). In citi bank a hacker from Russia hacked Citibank computer system in New York. The hacker transferred $10 million by hacking other accounts.

***Salami Attack***- Bank server is hacked; a small denomination of money may be Rs.1only will be deducted from all accounts and deposited to an opponent account. The amount is insignificant that neither the bank nor the account holder raise any concerns. For instance in (indiaforensic, n.a ; Maurya, 2014)USA a disgruntled bank employee after getting terminated developed a logic bomb into the bank’s systems which used to activate on every Saturday. He used to deduct ten cents from all the accounts in the bank.

***Denial of Service Attack-*** The most common attack on bank server is Denial of Service Attack. The prey's network is bombarded with spam mails which deprives him from using the services entitled to him or internet server is flooded with constant fake requests and not allowing authentic users to use the server or it crashes the server (Karim, 2016).

***Key loggers-*** Hackers and crackers design malicious software like Trojan (back door entry) and spread it globally via spam mail or links etc. The moment someone open that mail or link, the Trojan will infect the user system which will make the system prone to track and share the key moments such as user, account details etc. Software Key loggers are bit more expensive then hardware key loggers which are commercially available and are very inexpensive (Brar, 2012). The key logger attack can get easily plugged in any public computer by entering through the back door of the computer and can take the important data.

* 1. **SECURITY MEASURES**

Basic precautions are mentioned below from getting targeted or from becoming the victim (Alpna, 2016):

* + - Educate customers to use passwords by combining letters, numbers, and special characters, change them on regular intervals, and avoid sharing or disclosing them.
    - Secure your computer: regular updates of operating system is essential, keep updating the anti-

virus software, enable the firewall, block spyware attacks, ensure to check HTTPS rather than using just HTTP especially while transacting online and SSL/TLS protocols assures security. POST method is recommended instead of GET for sending information. Banks must use 2 factors or 3 factors Authentication check.

* + - Protect your data: Take regular backups of important data from pc, laptop, phone, tab etc. Protect

sensitive data by assigning a password to it. Allocate strong password to Wi-Fi (wireless) networks as they are prone to intrusion. Never share your credentials on phone or via emails. Don‘t revert or click a link or mail of an unknown user, check the source of the message; when in doubt, verify the source. Before making payment ensure that websites are secure, check for the padlock, https, etc.

# Counter Measures to Threats

* *Anti-Key Logging***:** The banks have implemented a great solution against key logging issue. Instead of keying in the credentials user can use virtual keyboard to protect them from falling in trap of

key loggers. Virtual keyboard will ensure security even on the compromised system as the mouse movement will be difficult to capture.

* *Anti-Hacking and Network Security***:** To safeguard the user the security solution must block the

illegitimate user or intruder not only at user’s end but also on kernel level. The users should install a good anti-virus and keep the system updated to cope with such attacks. A strong firewall should provide a better security by stopping illegal network communication (Kaur, 2015).

* *Anti-Phishing****-*** Phishing is possible because of many naïve and inexperienced users (Devarakonda,

2010). Therefore, it is recommended to train the users to recognize the fake or phishing site. Many banks and third party financial companies have initiated for the training. (Alnajim and Munro, 2009) research, is on analyzing the better way to retain anti-phishing knowledge, one way is to send the training material via email and the other is to give live demo classes. According to (Pathak, 2015) more security can be provided via two factor authentications i.e. one by checking login (user id and password) and other by image verification. The system will send a mail to the email-id given by the customer. She/he has to download that the image which will be in the .png format and share it at the bank website for the authentication purpose. The image will be less than 2^64 bits in length. The last 16 bits will be used to pass the security code for verification. This security code will be generated using MD5 (Message Digest 5), hashing algorithm.

* *Anti- Virus:* Users should install proper anti-virus software and keep updating it to refrain from

the attacks of malicious software’s and they can transact easily without any fear.

* *Biometrics:* Biometric has been derived from two Greek words Bio (life) and Metric is to measure. Biometric is extensively used in our laptops, mobile phones to provide better security. It can be categorized into two (Jain, 2011) Physiological (Face recognition, Fingerprint, Hand geometry,

Iris, Retina) and Behavioral Characteristics (Signature, Voice, Lip motion, DNA etc.). Biometrics is growing fast and is a good security solution (Fatima, 2011). Small handy devices like mobile, tabs, ipads etc.; biometric is a boon (Belkhede, 2012). Mobile payments will be very safe and no MITM attack or any such hacking is possible with the use of biometric as to copy or steal such traits is tough.

PNB (Punjab National Bank) has introduced two new services for securing the data

* + ***3D Secure Service***- It is an initiative by PNB which confirms user’s uniqueness via a simple check process while paying online. Bank issues a password to all his internet customers; similar to ATM- PIN for safeguarding the online transactions.
  + ***PNB IBS Shield***- It runs on a basic principle about customer remembering / logging on to his Bank's Internet site and not on any fake phishing site. It’s registration process covers the following steps.
    - Selecting a Picture from the Choices and categories of pictures offered to customer.
    - Entering a phrase/text ("PNB IBS Shield Phrase") easily recognized by the user.

HDFC Bank uses various methods to ensure secure online banking

* + **Login Security**: Net Banking account is accessible by an authentic customer who has an authentic Customer ID and IPIN (internet banking password, an arbitrarily generated pin). It is shared secretly with the customer and without entering the correct IPIN access is denied. The service will be canceled in case the user will not use it for more than 999 days.
  + **Session Security**: uses a 128-bit encryption to keep the transactions safe from hacking.
  + **VeriSign**: HDFC Bank's website is acknowledged by a digital certificate provided by VeriSign.

The customers’ can differentiate between phishing site and original bank site.

* + **Virtual Keyboard**: To secure the IPIN from software like key logger; which can be easily installed on global or public platform like cyber cafes; banks have offered virtual keyboard.
  + **Insta Alert**: Is a service to alert the customers by sending SMS/ Email on every transaction online or offline.

AXIS Bank is using NETSECURE, a double security system. It comes with very proficient security procedures for providing maximum safety to its account holders. It uses encryption and firewalls for safeguarding any distrustful attacks. **NETSECURE** is a two factor authentication method used for online security. The first parameter involves customer’s login credentials for accessing the site which includes id and password. The second parameter is a single-time password which is received by customer while conducting the transaction. Both of these parameters verify the customer’s identity. For transferring the funds online, it is obligatory to get registered for NETSECURE. While registering for NETSECURE

customer can opt for NETSECURE **with SMS, NETSECURE with Web Pin and NETSECURE with 1-Touch.**

ICICI Bank has initiated **I-SAFE**- At ICICI Bank, ease and safety of customer’s account is of utmost importance. In view of this, they have introduced "i-safe" an application which assures users about the online security. While transacting online 'i-safe' will generate (a six digit number) **One Time Password** (OTP) and send to the registered user via SMS/ e-mail. ICICI Bank for keeping itself away from the attacks and breaches; assures that online transaction should also remain safe while it is traversing from customer’s end to bank server. For ensuring this the bank login page has a password field which customer needs to input the password/pin (usually a 6 digit number) which automatically gets converted to a big number or bits the moment user press or click login. The original password now will not be retrieved by any intruder or hacker as data has expanded and now is a scrambled data.

* 1. **OSI ARCHITECTURE**

OSI Architecture is a systematic approach; an international standard ITU-T4 Recommendation X.800. The managers find it very useful to organize the task of providing security. Furthermore, this was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms. OSI Architecture (Stallings, 2011) should be followed to overcome the security issues. It highlights on Security attack, Security mechanism and Security services (Stallings, 2011; Krishna, 2009).

* + 1. *Security Attack****-*** which compromises on the safety of information. There are multiple ways through which intruder tries to get unauthorized information. Non-Cryptanalytic attacks are depicted in fig. 2.4; it is classified in two categories Passive and Active Attacks (Stallings, 2011; Denning, 1982).

=

***Passive Attack*** is passive in nature; here the attacker’s intention is to see or know the information without affecting system resources like eavesdropping or monitoring the transactions. Since no changes are made in the information or other resources, it's hard to trace such attacks. It is usually the attack on confidentiality. The primary focus is on anticipation rather than finding it; this could be easily barred using Symmetric Key Cryptography.

* *Message Contents*- Attacker A can read all messages sent by Mr. X to Mr. Y. For instance telephone conversation, email, file transfer (sensitive information).
* *Traffic Analysis*- Attacker A observes the pattern sent by Mr. X to Mr. Y. The opponent could see and trace all the exchanged messages and can track the frequency and length of messages.

***Active Attacks*** are opposite to passive attacks. As name suggests, these are active attacks which attempt to modify the resources and affect their operation by altering the data or creating a fake stream. They are tough to anticipate due to the vulnerabilities in hardware, network, and software. These attacks are on the integrity and availability of the data. Following are the Active attacks-

* *Masquerade*- when an entity plays to be someone else or different entity. For example, Mr. X sent a message to Mr. Y, but is hacked in between & altered by the opponent A and the message is resent to Mr.

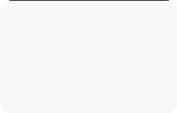
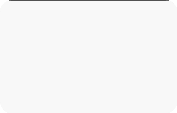
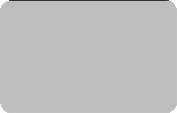
Y. After receiving the message, Mr. Y will feel the message is sent by Mr. X although the word is now deceived and sent via attacker A.

* *Replay* is acquiring the data passively and retransmitting it to produce an illicit effect. For instance, the message sent by Mr. X is transmitted to Mr. Y and simultaneously hacked by the attacker A. Later the opponent A alters and resends the message to Mr. Y portraying himself as Mr. X.
* *Modification of messages-* A change or alteration in a part of the legitimate message, or those messages are delayed or reordered, to create an illicit effect. For example, A message meaning “Meet me @ Café Coffee Day, 5 on coming Friday” is modified to say “Meet me @ Dominos, 5 on next Friday.”
* *Denial of service* prevents or inhibits the normal use of communications facilities. DOS/DDOS may suppress or overload all messages directed to a particular destination, to degrade the performance.
  + 1. *Security Service-* It is a method that improves the security of data processing to information transfer. The services are envisioned to counter safe the attacks; for which some security mechanisms to provide the service is used. These services are as follows: (Masram, 2014).
* *Accountability*- In case of some security breach pops up, actions can be tracked down or retrieve (Forouzan, 2010; Stallings, 2011).
* *Data Confidentiality*: Confidentiality of data means the information needs to be private; information might be on the system or while transmission of information. It guarantees that sensitive information will remain closed to an unauthorized user and should be read by only the intended receiver. In short, data confidentiality shields the data from any unauthentic user to view or access the data (Stallings, 2011). Symmetric Encryption works as a solution to attain confidentiality and privacy, Asymmetric key uses the concept of Digital Signature to confirm authenticity, availability, non-repudiation, integrity.
* *Privacy*: Assures the individual control of collecting and sharing the information by whom, and to whom. Privacy is attained by Symmetric Encryption (Forouzan, 2010; Stallings, 2011).
* *Authentication*: Identifies or verifies that the senders of messages are, in fact, who they claim to be and not some intruder or illegal or unauthentic person. Message & user can be authenticated by hash technique and digital signatures (Forouzan, 2010; Stallings, 2011).
* *Integrity:* Is satisfying the receiver that the message received is authentic and is not altered or tampered. In short, Information obtained should be original, complete, uncorrupted, unaltered or untemper. Integrity is achieved via hashing technique.
* *Non-repudiation:* While transacting online it is essential for both the parties to agree to the contract implied and should not back out or deny their obligations without being detected. This is attained by hashing or digital signature (Forouzan, 2010; Stallings, 2011).
* *Availability:* For an authentic user the information should be available (Forouzan, 2010; Stallings, 2011).
  + 1. *Security Mechanism -* A way to identify, stops, or recover from a security attack. Many security tools are there to provide safety. Various mechanisms are integrated into the appropriate protocol (OSI

security) layer and some are accepted globally. Security of all resources (system, network and data) is essential. System Security verifies that system is not affected by any malicious software. Network security should confirm the authentication access controls given to the individual user. (Application Layer PGP, HTTPS, SMIME, TCP Layer- SSL/ TLS, Firewall, IP Layer- IPV6, AH). Encryption is possible at any layer; the higher level it is implemented; it becomes more expensive but will provide better security. Data Security should safeguard the data from unauthentic user so that no unauthorized user can read the original message for which measures like Encryption, Message Digests, Digital Signatures, etc. are used.

For instance Encryption, Digital Signature, Traffic Padding, Routing Control, Notarization, Access Control, Data Integrity falls into the appropriate protocol layer category. Event Detection, Audit Trail, Security Recovery, etc. are Pervasive Security Mechanisms examples. Cryptography is a productive and useful mechanism to provide security (Scheneier, 1996; Park, 2007; Guo, 1999). Cryptography can handle various security services like Confidentiality, Integrity and Authentication. It is a subset of Cryptology.

* 1. **CRYPTOLOGY-** It is a science deals with the reading, writing and breaking of codes (Srinivasarao, 2011). It includes both cryptography and cryptanalysis as shown in figure 2.5. Its practitioners are called cryptologists.



Cryptology

Cryptography

CryptAnalysis

Fig. 2.5: Classification of Cryptology

***Cryptanalysts****-* Practitioners of cryptanalysis; who study how to compromise security mechanism. They deal with hacking the protected data, breaking the algorithm and retrieving the original message (plain Text). *Cryptanalysis* is a science of breaching Cipher text and seeing through the disguise.

* 1. **CRYPTOGRAPHY** –Cryptography is an amalgamation of two Greek words Kryptos (Secret/hidden) and Graphine (Writing) (Forouzan, 2008). It deals with writing secretly; the message is jumbled and no unauthorized user after breaching or hacking can access or retrieve the original message/ information/plain text. When it comes to security it is the essential and critical part which secures online transmission of information. It ensures security for communicating with insecure Channels (Agrawal, 2012). Cryptographers practice the sub-branch of Cryptology named as Cryptography used to design algorithms for encryption/ decryption. It is a process of transforming a message into a scrambled data (unreadable format) using various mathematical processes (Gupta, n.a).

As discussed about the cryptographic system in RFC 2828 (Edney, 2003), “it is a set of cryptographic algorithms along with the key that is used in some application context.” Cryptography was initially used by emperors, military, etc. but now it is used by everyone, every day. Whenever a mobile phone is used, an email is sent, a credit/debit/smart card is used, a secure website is browsed, iPod, iTunes, Kindle, VPN (Virtual Private Networks), etc. is used; cryptography is being used at the core to safeguard the data.

**Basic Terminology of Cryptography (Scheneier, 1996; Stallings, 2011)**

* + - Plain Text- The original or actual message sent by the sender.
    - Encryption- Is a technique implemented at sender’s end to ensure security. It’s an excellent and secure way to convert input (plain text) to output (cipher text) (message remains safe even on an insecure channel). The procedure involves an algorithm along with a key. Algorithm performs

substitution and transformation.

* + - Key- is the most important elements of cryptography process. It is used with encryption/decryption algorithm to exchange input (plain text) to output (cipher text) and vice versa. According to

Kerchoff, the system should be compromised only if the key is known to an unauthentic user. Hackers might know everything besides key, from the algorithm to cipher text; some plain text should not be able to access the message. As Key ensures security; key size and key selection are necessary for providing better security. Encryption algorithms can fall in two categories:- Symmetric Key (Single/Private Key) and Asymmetric Key (Public Key).

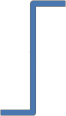
* + - Cipher text- A scrambled message after the algorithm is executed and Key, which makes it secure.

If the key is not authentic; message retrieved by a hacker is meaningless.

* + - Decryption- Is a way that executes at receiver’s end and that too in a reverse order, it uses

algorithm and key to decipher the output (cipher text) into plain text.

* + 1. Types of Cryptography**-** Cryptographic algorithms can be classified as Symmetric Key and Asymmetric Key as shown in fig 2.6:



DES

3DES

Block Cipher

AES

Symmetric Key Algorithms

IDEA

BlowFish

Stream Cipher RC4

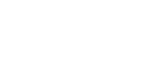
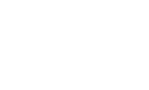
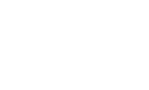
Cryptography

Asymmetric Key Algorithms

RSA ECC

Fig. 2.6: Types of Cryptography

* + - 1. *Asymmetric Key Encryption Algorithm-* A set of key is used, with the help of public key message will be broadcasted (sent after encrypting the message) and the private key will decipher it back to the original message. The concept of using two-keys was given by Diffie and Hellman, 1976. In this method every user has a pair of keys, one key he announces globally for communication, and one he keep safely (hidden from all) with him. The message could be broadcasted by anyone who knows the public key but the message could be decrypted or decoded by the one who possess the secret or private key. This provides integrity, authenticity and non-repudiation. Asymmetric key lacks privacy and confidentiality as anyone who possesses the public key can get to access the message easily.
      2. ‘For instance, data is sent by user X to user Y and hacker M hacked in between and he also possess the public key then he will be able to see the data sent by X.



Plain

Cipher Text

Recipie nt

Plain

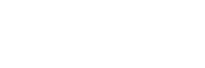
Sende

Encr-

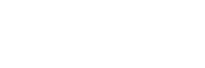
ypts

Decr-

ypts



Recipient’s Public Key



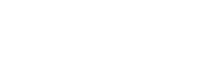
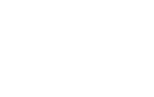
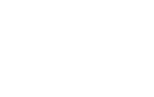
Recipient’s

Private Key

Fig. 2.7: Asymmetric Key Algorithm

* + - 1. *Symmetric Key Encryption Algorithm-* As depicted in fig. 2.8, same key or private key is shared between both sender and receiver of the message to encipher and decipher the code. It is also identified as a conventional /private/ secret key or standard encryption. The benefits of using symmetric over

asymmetric is its efficiency, speed, and less computational power. Symmetric key encryption provides data confidentiality and Privacy. In symmetric key, the key is shared safely in advance between sender- receiver. Symmetric key can be processed either in fixed blocks (block cipher) or bit by bit (Stream Cipher).



Plain

Cipher Text

Recipien

Same Key is shared

Plain

Sender

Encrypt

s

Decrypt

s

Fig. 2.8: Symmetric Key Algorithm (Scheneier, 1996; Stallings, 2011)

* + - * 1. Stream cipher- It accepts only one bit or sometimes single byte as an input/plain text. Key stream is infinite sequence of random bits (never reused). Few examples are RC4, Vernam Cipher, and One Time Password etc. Stream cipher can be classified in two ways:

Synchronous, a state is kept by the encryption algorithm but is not correlated with the plaintext or cipher text.

Self-synchronizing, in this some information (from the plaintext or cipher text) is passed to the operation of the cipher to intimate the cipher.

* + - * 1. Block cipher- it divides the message (M) into chunks of data or blocks of fixed size. This will break the input (plain text) message into same size with the help of key and produce cipher in the block form. The message is broken into equal size blocks. These blocks influences both security (block size should be large) and complexity (large block size is more costly to implement). Popular block algorithms are DES, AES, Blow fish etc.

*2.6.2* Algorithms Analysis: (Krishna, 2009) Different algorithms offers diverse level of security calculated on the basis of time taken to break or how difficult it is to breach. Algorithm is considered safe in few cases like: in case it is taking more time to breach the algorithm than the time that the enciphered code should remain secret. In case the cost incurred to break an algorithm is higher than the value of the encrypted data it is safe. Algorithm is secure if the amount of data encrypted with a single key is less than the amount of data necessary to break the algorithm.

To consider an algorithm totally safe; it should be difficult to find out the plain text despite of knowing substantial amount of cipher text. Brute Force Attack is an attempt to try exhaustively with all possibilities to retrieve meaningful data from the known cipher text. One time pad is evident in such circumstances as it is resilient for a cipher text only attack, simply by trying every possible key one by one and by checking whether the resulting input is meaningful. Cryptography is concerned with crypto systems that are computationally infeasible to break. Any algorithm is treated secure if it is unbreakable with available resources. The attack complexity can be measured in terms of data complexity, processing complexity etc. Data complexity deals with total data needed as input for the attack, processing complexity deals with the time needed to perform the attack and storage requirements which are the amount of memory needed to do the attack which is space complexity.

As a thumb rule, the complexity of an attack is taken to be least of these three factors:

* First it depends on the complexity and complication of the algorithm,
* Second is the complexity of the algorithm by its construction and
* The last is complexity of the algorithm by its strength.

By its construction, the time complexity of the algorithm can be calculated by executing through the steps of the algorithm, which will be referred as O (n). Complexities can also be expressed as orders of magnitude. If the length of the key is k, then the processing complexity is given by 2^k. It means that 2^k operations are required to break the algorithm. Then the complexity of the algorithm is said to be exponential in nature.

An essential resource of an encryption algorithm is a change in a single bit in the input or in key which should transitively affect the output with a radical change in cipher text. This is named as avalanche or Butterfly effect. The more the change is, the better the security. Cryptanalysis is a way to recover the input

without knowing the key. It may also find weakness in the system that identifies patterns which can be useful in knowing the previous results.

Cryptanalysis is done to breach the algorithm and recover the plain text. People or statistician involved in statistically breaching the code and getting either the key or Plain text are called Cryptanalysts.

* 1. **CRYPTANALYSIS**- The basic idea of cryptography is to shield the message / input (plain text) from attackers or adversaries. It is anticipated that the opponent knows the complete communication between both parties (sender and receiver). Cryptanalysis uses techniques without being aware of the key to break the message. In nineteenth century, a Dutch cryptographer; Kerchhoff laid a principal that “A cryptosystem should be safe even if the attacker knows the details about the system, with the exception of the secret key. Any unauthorized user, if by any chance hack the data should not be able to see the authentic message until he possess a key with him” (Stallings, 2011).
     1. Types of *Cryptanalytic* Attacks: (Denning, 1982; Schneier, 1995; Stallings, 2011; Sekar, 2011; Krishna, 2009; Forouzan, 2016*). Assumption:* Encryption algorithm is known to the eavesdropper/intruder.
        + Cipher text-only: Only intercepted cipher-text is available to hacker (Cipher text)
        + Known-plaintext attack: Some plaintext/cipher-text pairs for the current key are accessible. (Cipher text, One or more plaintext-cipher text pairs formed with secret keys)
        + Chosen-plaintext attack: cipher text relative to any specified message (Plain Text) for current key

is accessible to the hacker (Cipher text, Plaintext message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key)

* + - * Chosen-cipher text attack: Partial data is gathered, by choosing (cipher-text) an output and

receiving its deciphered data beneath an unknown key (Cipher text, Cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key).

* + - * Chosen-text attack: Is a blend of choosen plain-text and chosen cipher-text attack (Cipher text,

Plaintext message chosen by cryptanalyst, together with its corresponding cipher text generated

with the secret key, Cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret Key.)

* Brute-force attack: Is a passive attack, will perform an exhaustive search for cracking the key.

Exhaustive search means computing all probable arrangement that could give a plain text (message or password) and test it to verify if the password is correct.

* Dictionary attack: Is like brute force attack as the trespasser is able to rank keys (in order of

probability like most probable, least probable etc.) and compile a list of the most probable (the dictionary), and test them in that sequence.

* Timing attack: Timing attacks is a side channel attack which enables an intruder to fetch the secrets

kept in a security system by noticing the time it takes the system to reply to various queries.

* Man-in-the-middle attack: MITM, an active attack as an eavesdropper controls the entire conversation. In MITM, the two authentic parties believe that they are communicating directly to each other in a safe environment without noticing that a hacker is secretly reading and perhaps

changing the data.

**CHAPTER 3**

# **PROPOSED METHODOLOGY**

**Background and Motivation**

The banking sector has increasingly faced security challenges in managing online transactions, particularly in preventing fraud, unauthorized access, and data breaches. Traditional banking systems, while efficient, struggle with issues related to centralization, which creates single points of failure, making them vulnerable to cyberattacks. The **Secure Banking Using Blockchain** project leverages blockchain’s decentralized, immutable, and transparent ledger system to address these security concerns. Blockchain technology has the potential to revolutionize the banking sector by ensuring data integrity, securing transactions, and reducing the risks associated with centralization.

**Objectives**

The primary objective of this project is to design and implement a blockchain-based banking system that enhances transaction security and reduces the risks of fraud and data manipulation. The system aims to:

* Secure banking transactions through decentralized architecture.
* Provide transparency for all stakeholders by recording transactions on a public ledger.
* Ensure the authenticity and integrity of data through cryptographic encryption.
* Automate processes to improve efficiency and reduce human errors.

**Scope**

This project focuses on building a secure banking system prototype using blockchain technology, utilizing tools such as **Ganache** for creating a local blockchain environment and **MetaMask** for wallet integration and transaction signing. The system will include features like encrypted transactions, smart contracts, and peer-to-peer (P2P) verification, providing a scalable and secure banking solution.

**Blockchain Fundamentals and Relevance**

**Blockchain Technology Overview**

Blockchain is a distributed ledger technology that securely records transactions across multiple nodes in a network. Each transaction is encrypted and linked to the previous one, creating a chain of blocks that are resistant to alteration. This structure ensures the integrity and security of data, making it particularly suitable for industries like banking, where transparency and immutability are critical.

**Benefits of Blockchain in Banking**

The characteristics of blockchain make it ideal for enhancing banking security:

* **Immutability**: Once recorded, data cannot be altered, creating a tamper-proof ledger.
* **Decentralization**: By eliminating the need for a central authority, blockchain reduces risks related to centralized systems, such as fraud and unauthorized access.
* **Transparency**: All stakeholders can view the ledger in real-time, fostering trust and accountability.
* **Cryptographic Security**: Each transaction is encrypted, ensuring the confidentiality and authenticity of data.

**Introduction to Blockchain in Banking**

Blockchain technology has introduced a new paradigm for secure financial transactions. By providing a decentralized, transparent, and immutable ledger, blockchain addresses several long-standing challenges faced by the banking sector, including fraud, hacking, and data breaches. In this project, blockchain is used to develop a secure banking platform that protects sensitive data and secures transactions. The system uses **Ganache** as a local Ethereum blockchain simulator and **MetaMask** as a digital wallet for secure transaction signing and verification.

**Overview of the Proposed System Architecture**

The proposed blockchain-based banking system is designed to provide a secure and efficient environment for processing transactions. The architecture is divided into several components:

* **Blockchain Network**: A private Ethereum blockchain network, simulated using **Ganache**, serves as the backbone of the system. It records and stores all transaction data, ensuring transparency and security.
* **Smart Contracts**: Smart contracts automate various banking processes, such as executing transactions, verifying identities, and enforcing compliance with security protocols.
* **MetaMask Wallet**: **MetaMask** acts as the interface between users and the blockchain network. It is used for signing and executing transactions securely, ensuring that only authorized users can access the system.
* **Web Application**: A web-based interface allows users such as bankers and customers to interact with the system securely. It provides modules for account management, transaction monitoring, and auditing.

**System Design and Development**

The development of the secure banking system follows a structured approach involving several phases: requirement analysis, system design, smart contract development, web application development, and testing.

**Requirement Analysis**

This phase involves understanding the key security challenges of traditional banking systems and identifying how blockchain can resolve these issues. The following requirements were identified:

* **Authentication and Authorization**: Ensure that only authorized users can access or modify data.
* **Transaction Security**: Provide end-to-end encryption and immutability for all transactions.
* **Data Privacy**: Protect sensitive customer information through cryptographic methods.
* **Regulatory Compliance**: Ensure the system complies with banking regulations and financial standards.

**System Design**

Based on the requirements, the system’s architecture is divided into the following layers:

* **Blockchain Layer**: The private Ethereum blockchain simulated using **Ganache** stores transaction data.
* **Smart Contract Layer**: Smart contracts manage transaction processes, such as identity verification and fund transfers.
* **Application Layer**: A web-based application provides the user interface for interacting with the blockchain.
* **Integration Layer**: This layer consists of APIs that enable communication between the web application, MetaMask wallet, and the blockchain.

**Smart Contract Development**

Smart contracts are written in **Solidity**, the primary programming language for developing smart contracts on Ethereum. The contracts automate core banking operations such as:

* **Transaction Processing**: Securing and recording every transaction on the blockchain.
* **Identity Verification**: Verifying user credentials and ensuring that only authenticated users can access their accounts.
* **Compliance Checking**: Ensuring that every transaction complies with banking regulations.

Each smart contract is tested using the **Truffle** framework to ensure that it functions as intended and is secure before being deployed on the blockchain network.

**Web Application Development**

The web application is developed using **React.js** to provide a user-friendly interface for customers and banking staff. The application is designed to handle:

* **Customer Module**: Allows customers to manage accounts, view transaction history, and initiate transactions.
* **Banker Module**: Enables bank staff to verify transactions, monitor security issues, and manage customer accounts.
* **Admin Module**: Provides system administrators with tools to oversee the entire system, ensuring compliance and security.

The application integrates with **MetaMask** to securely sign and manage transactions.

**Implementation and Deployment**

The implementation of the medicine supply chain management system involves deploying the smart contracts on the private Ethereum blockchain network and hosting the web application on a web server.

**Ganache Setup**

Ganache is set up to simulate a private Ethereum blockchain network on a local machine. It provides a graphical interface for managing accounts, viewing transactions, and monitoring smart contract events. The blockchain network is configured to have multiple accounts, each representing a different stakeholder in the supply chain, such as manufacturers, distributors, pharmacists, and consumers.

**Smart Contract Deployment**

The smart contracts are deployed on the Ganache blockchain network using the Truffle framework. Truffle provides a suite of tools for compiling, deploying, and managing smart contracts. The deployment script is configured to deploy all the smart contracts to the blockchain network and initialize them with the necessary data.

**MetaMask Integration**

MetaMask is integrated with the web application to provide a secure and convenient way for users to interact with the blockchain network. Users are required to install the MetaMask extension in their browser and create a wallet. The web application is configured to connect to the Ganache blockchain network using MetaMask, allowing users to sign transactions and execute smart contracts.

**Web Application Deployment**

The web application is deployed on a web server using a platform-as-a-service (PaaS) provider, such as Heroku or AWS Elastic Beanstalk. The application is configured to connect to the Ganache blockchain network using Web3.js, a JavaScript library for interacting with the Ethereum blockchain. The deployment process involves building the application, configuring environment variables, and setting up a domain name.

**Testing and Evaluation**

The final phase involves testing and evaluating the system to ensure that it meets the requirements and functions as expected.

**Functional Testing**

Functional testing is conducted to verify that each component of the system functions correctly. This includes testing the smart contracts to ensure that they execute as expected, testing the web application to ensure that it provides the correct user interface, and testing the integration with MetaMask to ensure that transactions are signed and executed correctly.

**Security Testing**

Security testing is conducted to identify and address any vulnerabilities in the system. This includes testing the smart contracts for common vulnerabilities, such as reentrancy and integer overflow, testing the web application for vulnerabilities, such as cross-site scripting (XSS) and SQL injection, and testing the integration with MetaMask to ensure that sensitive data is not exposed.

**Performance Testing**

Performance testing is conducted to evaluate the system's scalability and performance under different loads. This includes testing the blockchain network to ensure that it can handle a large number of transactions, testing the smart contracts to ensure that they execute efficiently, and testing the web application to ensure that it responds quickly to user requests.

# Analysis and discussion

This chapter analyzes and discusses the literature review from the previous chapter, focusing on the role of trust and transparency in blockchain-based banking systems. It then delves into how blockchain technology is applied to banking transactions and concludes with an analysis of its limitations and strengths.

#### 2.1 Trust

The 2017 Edelman Trust Barometer found that trust in institutions, including NGOs and corporations, declined to record lows in 2016, comparable to levels seen during the financial crisis. In fact, 85% of respondents expressed distrust in the system, with only 52% indicating they trusted businesses (Edelman 2017).

How can trust be regained in a banking system? Blockchain technology offers a solution by ensuring trust through mathematics, cryptography, and decentralized verification of transactions. Blockchain can resolve issues related to multiple parties with conflicting interests without human intervention. Disputes that arise from mistrust can be minimized when blockchain replaces traditional centralized systems because it is self-executing, administrator-free, and decentralized.

In a blockchain-based banking system, transactions are not controlled by a central authority, which could potentially manipulate the system. Instead, blockchain provides a decentralized, transparent, and trusted way to manage ownership and transaction records. When parties have conflicting interests about who owns what, blockchain eliminates the need for intermediaries, such as banks, by embedding trust into the system itself. Trust is no longer placed in central institutions but rather distributed across the blockchain network. Peer-to-peer networks replace central authorities, and no single entity can unilaterally take action on behalf of the community. This decentralization fosters trust in the system and prevents institutions from defying community rules, enhancing the overall reliability of the system (Sun et al. 2016).

#### 2.2 Transparency

Blockchain technology can significantly improve transparency in banking by maintaining a decentralized ledger that records and tracks every transaction. Every participant in the blockchain network has an updated copy of the ledger, enabling real-time monitoring and auditing of transactions. In a banking context, this transparency allows for real-time verification of the provenance of funds, ownership, and transaction history.

Additionally, blockchain-based smart contracts can safeguard information privacy by providing secure, access-controlled environments. Individuals and entities can be granted specific permissions, regulated by smart contracts, to access certain information in the system. These access controls are determined by the owner of the data, ensuring that no third party can access private information without authorization.

In a blockchain-enabled banking system, customers can view the complete history of their transactions, from the initial deposit to the final transaction. This transparency is especially critical in scenarios where trust in traditional financial institutions has eroded. By utilizing blockchain, banks can offer an unparalleled level of transparency and trust, which could also provide a competitive advantage in the future as customers demand greater transparency in their financial dealings.

### 4.3 Blockchain in Banking Systems

Blockchain has the potential to revolutionize the banking system by offering secure, transparent, and trusted technology solutions. One such application is registering and validating all transactions on a blockchain, which records key details such as parties involved, transaction amounts, dates, and other relevant data.

The decentralized and public nature of blockchain ensures that every step of a transaction is transparent and traceable, making it nearly impossible for malicious actors to tamper with the data. This also prevents central authorities or hackers from taking control of the blockchain to manipulate transactions.

Smart contracts on the blockchain can further automate banking processes. For example, payments can be triggered automatically when certain conditions, such as the fulfillment of a service or delivery of goods, are met. This can streamline operations and reduce the reliance on intermediaries.

#### 4.3.2 Transactions

Blockchain technology is particularly ideal for transactions between two or more parties. It allows for secure, open, peer-to-peer transactions that can be verified and audited by any participant in the network. Unlike traditional banking systems that rely on intermediaries and manual verification, blockchain transactions are recorded and settled almost instantly, making them more efficient.

Paper-based and electronic banking systems, which rely on double-entry accounting and centralized record-keeping, are often inefficient and susceptible to tampering. Blockchain’s decentralized structure eliminates the need for trust in intermediaries, allowing for faster, more secure transactions. Furthermore, every participant in the network has access to a full, auditable history of all transactions, making the system transparent and accountable.

Traditional banking transactions often require third-party intermediaries, such as banks or clearinghouses, to process payments and manage records. Blockchain eliminates the need for these intermediaries by providing a higher degree of trust through automated, smart contract-based systems. These smart contracts can handle complex transactions without requiring human oversight, which is particularly useful in scenarios where trust in financial institutions is low (Edelman 2017).

### 4.4 Limitations and Strengths of Blockchain Systems

While blockchain technology has the potential to enhance trust and transparency in banking, it does not inherently address the reliability of the records it maintains. The accuracy of the data entered into the blockchain depends on the integrity of the individuals or systems entering the information. For example, in scenarios where a third party records a transaction, they could enter fraudulent or misleading data, which would then be permanently stored on the blockchain.

Blockchain’s primary strength lies in its ability to maintain the authenticity and integrity of records through cryptographic security and decentralization. While no system is entirely immune to attacks, blockchain is one of the most secure technologies ever designed (Nakamoto 2008). Ensuring the reliability of the data entered into the blockchain remains a challenge, but its potential to revolutionize banking through decentralized trust and transparency is undeniable.

**INPUT DESIGN AND OUTPUT DESIGN**

**INPUT DESIGN**

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

* What data should be given as input?
* How the data should be arranged or coded?
* The dialog to guide the operating personnel in providing input.
* Methods for preparing input validations and steps to follow when error occur.

**OBJECTIVES**

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

**OUTPUT DESIGN**

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

* Convey information about past activities, current status or projections of the
* Future.
* Signal important events, opportunities, problems, or warnings.
* Trigger an action.
* Confirm an action.

**SYSTEM STUDY**

**FEASIBILITY STUDY**

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

* ECONOMICAL FEASIBILITY
* TECHNICAL FEASIBILITY
* SOCIAL FEASIBILITY

**ECONOMICAL FEASIBILITY**

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

### TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

**SOCIAL FEASIBILITY**

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

**OPERATIONAL FEASIBILITY**

Operational feasibility is the measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.[[14]](https://en.wikipedia.org/wiki/Feasibility_study#cite_note-SAD-Global_Enterprise-14)

The operational feasibility assessment focuses on the degree to which the proposed development project fits in with the existing business environment and objectives with regard to development schedule, delivery date, [corporate culture](https://en.wikipedia.org/wiki/Corporate_culture) and existing business processes.

To ensure success, desired operational outcomes must be imparted during design and development. These include such design-dependent parameters as reliability, maintainability, supportability, usability, producibility, disposability, sustainability, affordability and others. These parameters are required to be considered at the early stages of design if desired operational behaviours are to be realised. A system design and development requires appropriate and timely application of engineering and management efforts to meet the previously mentioned parameters. A system may serve its intended purpose most effectively when its technical and operating characteristics are engineered into the design. Therefore, operational feasibility is a critical aspect of systems engineering that needs to be an integral part of the early design phases.

# **CONCLUSION**

The implementation of blockchain technology in the banking sector has the potential to significantly enhance the security, transparency, and efficiency of financial transactions. By decentralizing the management of transactions and removing the need for trusted third-party intermediaries, blockchain introduces a new level of trust through its cryptographic security, distributed ledger, and immutable record-keeping.

In this project, **secure banking using blockchain** was demonstrated as a viable solution for addressing the shortcomings of traditional banking systems, such as inefficiencies, high operational costs, data breaches, and mistrust in centralized institutions. Blockchain ensures that each transaction is verified, transparent, and secure, eliminating the possibility of tampering or fraud. Furthermore, the introduction of smart contracts can automate complex banking operations, improving operational efficiency and reducing the need for human intervention.

Despite the significant benefits, the technology is not without its limitations. Challenges such as ensuring the accuracy of the initial data input, potential vulnerabilities in smart contract programming, and scalability issues must be addressed before blockchain can be fully integrated into mainstream banking systems. However, as advancements continue, blockchain’s capability to deliver secure, real-time, and auditable transactions could revolutionize banking and redefine how trust is established in financial services.

In conclusion, blockchain technology presents a transformative opportunity for secure banking, fostering a future where financial transactions are more transparent, secure, and efficient. With continued innovation and collaboration in this field, blockchain could play a critical role in shaping the future of banking and restoring trust in the financial system.

# **REFERENCES**

 Nakamoto, S. (2008). **Bitcoin: A Peer-to-Peer Electronic Cash System**. Retrieved from https://bitcoin.org/bitcoin.pdf

 Tapscott, D., & Tapscott, A. (2016). **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**. Penguin Books.

 Mougayar, W. (2016). **The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology**. Wiley.

 Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**. Proceedings of the 2017 IEEE International Congress on Big Data, 557-564.

 Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). **A Survey on Security and Privacy Issues of Bitcoin**. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452.

 De Meijer, C. (2020). **The Future of Banking: Blockchain Technology Could Rebuild the Banking System**. Journal of Digital Banking, 4(1), 1-14.

 Treleaven, P., Brown, R., & Yang, D. (2017). **Blockchain Technology in Finance**. Computer, 50(9), 14-17.

 Kshetri, N. (2017). **Will Blockchain Emerge as a Tool to Break the Poverty Chain in the Global South?** Third World Quarterly, 38(8), 1710-1732.

 Pilkington, M. (2016). **Blockchain Technology: Principles and Applications**. In Research Handbook on Digital Transformations, 225-253. Edward Elgar Publishing.

 Underwood, S. (2016). **Blockchain Beyond Bitcoin**. Communications of the ACM, 59(11), 15-17.

 Eyal, I., & Sirer, E. G. (2014). **Majority Is Not Enough: Bitcoin Mining Is Vulnerable**. Communications of the ACM, 61(7), 95-102.

 Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**. Princeton University Press.

 Buterin, V. (2013). **Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform**. Retrieved from <https://ethereum.org>

 Guo, Y., & Liang, C. (2016). **Blockchain Application and Outlook in the Banking Industry**. Financial Innovation, 2(1), 24-35.

 Dwyer, G. (2015). **The Economics of Bitcoin and Similar Private Digital Currencies**. Journal of Financial Stability, 17, 81-91.

 Schilling, L., & Uhlig, H. (2019). **Some Simple Bitcoin Economics**. Journal of Monetary Economics, 106, 16-26.

 Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). **The Economics of Digital Currencies**. Bank of England Quarterly Bulletin, Q3, 276-286.

 Christidis, K., & Devetsikiotis, M. (2016). **Blockchains and Smart Contracts for the Internet of Things**. IEEE Access, 4, 2292-2303.

 Tapscott, D., & Tapscott, A. (2017). **How Blockchain is Changing Finance**. Harvard Business Review. Retrieved from <https://hbr.org>

 Yermack, D. (2017). **Corporate Governance and Blockchains**. Review of Finance, 21(1), 7-31.