Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5, 1204-1220
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i5.7124

Data privacy in blockchain management scheme with Nudge Theory for banking sector

Dhanalakshmi Komatiguntala[1], Padmapriya Kota[2], Deepika Krishnan[3], Andalu Kongari[4], Sundari Dadhabai[5], Ravi Kumar Bommisetti[6*]
[1]School of Business and Management, Christ University Yeswanthpur Campus, Bangalore, India; dhanalakshmi.k@christuniversity.in (D.K.).
[2]Radhekrishna Women's College, Hyderabad, India; padmapriya.1410@gmail.com (P.K.).
[3]Symbiosis School of Banking and Finance, Symbiosis International University, Pune – 412115, India; krizdeepz@gmail.com (D.K.).
[4]Department of Commerce, TGSWRDC Vikarabad, India; gujjari.andalu@gmail.com (A.K.).
[5]KL Business School, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Andhra Pradesh 522302, India; sundaridadhabai@kluniversity.in (S.D.).
[6]Independent Researcher - Andhra Pradesh, India; ravi9949418650@yahoo.com (R.K.B.).

Abstract: Blockchain is an emerging digital transformation technique for processing and storing information. The study explores how blockchain technology can transform the banking sector by improving efficiency, transparency, and security. The main goal is to understand how blockchain can modernize traditional banking operations and address key challenges such as fraud, high transaction costs, and slow processing times. The study uses a qualitative approach, drawing insights from existing research, real-world examples, and current trends in financial technology. Findings show that blockchain offers clear advantages, including faster and more secure transactions, reduced operational costs, and improved record-keeping. It holds strong potential in areas like payments, trade finance, and compliance. However, the paper also highlights significant obstacles such as unclear regulations, difficulties in integrating with existing systems, and technical limitations related to scalability and interoperability. Blockchain is seen as a promising solution for many of the inefficiencies in current banking practices. Still, successful implementation will require careful planning, regulatory support, and collaboration across the financial ecosystem. The study offers practical insights for banks, technology developers, and regulators, recommending a gradual and strategic approach to blockchain adoption to ensure long-term value and sustainability.

Keywords: *Banking, Blockchain, Homomorphic, Nudge theory, Privacy.*

1. Introduction

The era of the big data banking sector exhibits the drastic utilization of digital transformation to withstand user requirements through digital services [1]. Also, with digital information banking sector exhibits faster and better experiences for the customers. The banking sector is highly engaged in "Open Banking" to offer customer benefits for effective data sharing and cooperation in the financial institutions [2]. The core data in the financial institutions are connected based on the perspectives of the stakeholders subjected to a vast range of difficulties and issues. However, the banking sector demands increased privacy concerns for owners for data sharing and information exchange to prevent fraud and abuse of data [3]. Additionally, data personal ownership and privacy are significant contributions to the field of open banking. The process of giving third-party payment platforms and financial service provider's access to consumer banking information such as transactions and late payments are known as open banking. Blockchain can help RTGS develop, enhancing the security of

History: Received: 12 March 2025; Revised: 4 May 2025; Accepted: 7 May 2025; Published: 13 May 2025
* Correspondence: ravi9949418650@yahoo.com

electronic transfers and minimizing the chances of accounting errors, misunderstanding, double accounting, and fraud. Accountants and auditors are excellent examples of businesses that are set to be disrupted by Blockchain. Blockchain is a network of peer-to-peer nodes that stores transaction data, also called blocks, of the public in several databases, also referred to as the "chain." This type of store is usually referred to as a 'public blockchain.' Especially, as the regulation provided in May 2018 came enforced as the General Data Protection Regulation (GDPR) by the European Union (EU). The General Data Protection Regulation is the world's toughest stringent privacy and safety law. Even though it was developed and passed by the European Union (EU), it imposes obligations on businesses anywhere else that target or collect data on EU citizens. The GDPR's goal is to impose a uniform data security law on all EU members, removing the need for each member state to write its own data protection rules and guaranteeing that laws are uniform across the EU. In consideration of challenges, companies of banks and financial technologies explored new emerging technologies compared to existing technologies in terms of the provision of services, products with regulation, and requirement for data privacy [4].

Blockchain is considered an emerging technology with effective growth to manage records in the list for peer-to-peer (P2P) networks in different fields such as cloud computing, Artificial intelligence, Internet of Things (IoT), big data, and so on [5]. Cloud computing refers to the on-demand usage of computer operating systems, especially data storage and computational power, without users trying to handle them personally. Functions in larger clouds are often distributed across numerous locations, each one is a data center. Artificial intelligence is the capacity of a computer or a robot controlled by a computer to do human tasks with intelligence and discernment. Peer-to-peer networks are typically made up of a handful or fewer computers. These computers individually store their data with their very own security, and they also share information with the entire network. Peer-to-peer networks contain nodes that both receive and give resources. In a peer-to-peer network, the computers on the network are considered equal, so each computer has access to the same opportunities and data. This is a basic network wherein computers can communicate with each other and exchange what's on or connected to their computers with other users. Blockchain secure run-in computation of the one in which the owner of the raw data has significant access. Recently, with increased interest and effort in the application of the blockchain and smart technologies in different areas such as insurance, government, education, medical application, digital storage, and electricity [6].

Although blockchain technology is considered a key enabling technology for data security and privacy [7]. Using decentralized identification and other security features, blockchain and public blockchain technology offer novel opportunities for safeguarding user data. These technologies can give consumers greater control over their data by offering tools to allow them to own and control it. Blockchain is decentralized, encoded, and cross-checked, the information may be believed. Since the blockchain is so tightly populated with nodes, accessing the majority of nodes at the same moment is difficult. However, blockchain is subjected to certain limitations for financial data in terms of privacy preservation in granularity for customer data that are not suitable for existing bank applications and limited information for their data [8]. Another limitation of blockchain is the limited utilization of information data and data complexity and variety in the bank sub-system to deal with customer data authorization for tedious operations. With conventional laws and regulations, effective management of bank operations and customer data needs to be managed.

This paper developed a secure framework model for the black chain process in bank operations. The estimation is based on the ledger operation of the banks with consideration of the blockchain security scheme. The proposed security model comprises the homomorphic process integrated with the Nudge model. Within the Nudge-based model collaborative filtering is applied for processing. Collaborative filtering refers to the set of algorithms that include several methods for finding similar users or items, and also multiple methods to calculate ratings based on ratings of similar users. You might end up with a collaborative filtering technique based on your choices. Collaborative filtering refers to the set of algorithms that include multiple methods for finding similar users or items, and multiple methods to

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

calculate ratings based on ratings of similar users. Collaborative filtering is a system that correlates this user's ratings to other users and finds those with the most "similar" tastes. The developed security model framework is implemented and evaluated for the authentication and security aspects based on the consideration of the decryption and encryption of the data. When one of the participants adds a new data item to the blockchain, the first uses the private key to uniformly, encrypt it. The operation is then submitted to the blockchain with encrypted data. The paper is organized as follows: the review of blockchain technology in the banks is presented in section 2. In Section 3 developed secure framework model for blockchain technology in the banks is presented based on the characteristics of banks and customers. Section 4 provides the experimental evaluation of the developed security model, followed by an overall conclusion in Section 5.

2. Related Works

The study reveals that non-performing loans (NPLs) in Cyprus are largely influenced by both borrower-specific factors—such as age, gender, education, and financial standing—and broader economic conditions, including inflation, interest rates, and unemployment. Inadequate lending practices and insufficient borrower evaluations were found to contribute to early repayment difficulties and elevated credit risk [9]. The study shows that the proposed load-adaptive cross-chain control method significantly enhances the performance of Blockchain IoT systems. Notable improvements include more effective load balancing, reduced communication overhead, better use of resources, lower transaction delays, and increased energy efficiency. These benefits make the solution highly suitable for complex, high-traffic environments such as ports [10]. The proposed framework effectively combines federated learning, LSTM auto encoders, and CNNs with blockchain technology to improve transaction security, transparency, and fraud detection. It demonstrated high accuracy (94.5%), strong detection performance (F1-score of 96.7%), and faster model validation (120 ms), while ensuring robust data privacy and efficient resource usage compared to existing methods [11]. This study introduces a secure e-voting system that combines AES, RSA encryption, and blockchain technology to strengthen data privacy, accuracy, and integrity in digital elections. The system demonstrated rapid encryption (0.068ms) and decryption (0.054ms) speeds with 4096-bit keys, surpassing traditional methods. It effectively minimizes vote mismatches, enhances overall reliability, and promotes the global potential for secure, transparent, and trustworthy digital voting processes [12]. The study introduces an optimization approach for virtual power plants (VPPs) that aggregate multiple microgrids (MMGs) using blockchain technology. It implements a priority-based auction system and a penalty for malicious bids to help reduce costs and prevent dishonest practices. Additionally, it ensures the privacy of transaction prices, promoting fairness and efficiency in energy market operations [13].

The study finds that integrating blockchain with cloud technologies significantly enhances financial security in national health insurance by reducing fraud, improving data privacy, and increasing transparency. However, successful implementation requires addressing integration challenges, regulatory compliance, and encouraging technological adoption across existing healthcare financial systems [14]. The potential application of blockchain technology in the banking industry was explored by The potential of blockchain in banking was explored by Vernekar, et al. [15] emphasizing enhanced security, transparency, and efficiency. Fraud and costs are expected to decline, though challenges in regulatory compliance and technical infrastructure remain. Nonetheless, blockchain is viewed as transformative for traditional financial systems despite these hurdles. The integration of mobile banking, digital payment systems, and smart contracts into a blockchain-based financial system was examined by Hasan and Habib [16]. It was found that blockchain enhances transaction security, efficiency, and transparency while reducing costs and promoting financial inclusion. However, regulatory challenges and limited adoption were identified as barriers to fully realizing these transformative benefits. A blockchain-based solution was developed to enhance data integration, security, and transparency in financial institutions. The system ensures tamper-proof, efficient information sharing, reducing redundancy and improving accuracy. Despite integration challenges and

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

technical demands, its transformative potential in financial information management was highlighted by the study conducted by Xue [17]. This study presents a blockchain-based data privacy management framework tailored for the financial sector, particularly open banking. It introduces a data classification method, a collaborative filtering model, and a Nudge Theory-based disclosure scheme. Experimental results confirm the framework effectively enhances customer data privacy management in real-world banking environments [18].

Blockchain comprises the electronic scheme to withstand two issues such as problems with double payment and general problems [7]. In case of double payment, the decentralized system is eliminated from the local agencies that are engaged in the verification of the nodes that are distributed and the mechanism to consensus for the accomplishment of the value transfer process involved in the transmission of information [19]. The key application of blockchain technology is a smart contract for self-execution and an autonomous computing scheme to facilitate the agreements and performance between two parties. However, the application of the smart contract is available to a large extent to provide significant security performance based on the contract law with minimized transaction costs for negotiation, agreement, and verification process [20].

Blockchain is categorized into two categories such as public or permission blockchain through Bitcoin and blockchain permission with hyper ledger. Hyper ledger is an open-source platform that enables the construction of distributed ledgers based on blockchain. Hyper ledger is a group of people who work together to create the frameworks, standards, technologies, and libraries required to build blockchain applications and related applications. The major difference in the approach is variation in the ledger security scheme with a consensus algorithm. In a permission-based blockchain scheme without any specific identity, anyone can able to participate in the verification process of the block with a consensus created [21]. The blockchain-based permission is actively engaged in cryptocurrency but it provides higher latency in the generation of the blocks [22]. In blockchain with permission-based contributions on the system state consensus to offer, secure interaction between group entities without any trust to exchange business funds, goods, or information. Based on peer identity relay permission blockchain uses Byzantine-fault tolerant (BFT) [23] RAFT, or Paxos consensus. The ability of a computer network to continue operating even though some of its nodes fail or act maliciously is known as the Fault of Byzantine tolerance. The term comes from the Byzantium Generals Problem, a hypothetical.

Blockchain-based technology offers an effective solution for multiple data privacy schemes and open banking mechanisms for different application contexts [24]. In general, data privacy relates to a person's ability to choose when, how, and to what degree personal information to is shared with or communicated to others. The primary application is the peer – to peer transaction for cross-border payments and remittances in the transactions. Secondly, the blockchain-based approach uses reliable databases to provide information-based records with the characteristics of traceability and credibility in terms of anti-money laundering information schemes [25]. Thirdly, the rights confirmation, land ownership, contracts equity authentication to transfer and verification. The fourth scenario with the blockchain is intelligent management in the smart contract that can be automatically detected and conditions are triggered [26]. In this contract, information is automatically processed with the automated payment processing, profit of participation and so on. However, blockchain data facilitates access to the original user to read the data and other users who need the authorization to access the data, and management of data privacy [27]. The limitations associated with the blockchain authentication-based secure framework model are listed as follows [28]:

1. With the technology of big data analysis public keys can be easily located by those actively engaged in the big transaction and identify the public key owner based on transaction time and information about banks and so on.

2. Based on GDPR values the data about companies' data need to be deleted completely to gather the requirements of citizens to eliminate data. At present, the companies or banks that use blockchain

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

technology information elimination is based on consideration of conditions and situation without any clear rules.

3. As per the Data Protection Act the design of banks needs to be redesigned with the adoption of collaborative work between application and blockchain technology framework. Also, the customers of the banks need to confirm the scheme for data disclosure.

4. According to the GDPR act, personal data provides identifiable information about living or data type by the customer in a different scenario. Based on that customers can activate or close one personal account with the elimination of all relevant data copies with the sharing of a complete banking scenario. With data strategy management and privacy schemes, different banks are provided with the smart ledger. Mutual distributed ledgers are also known as smart ledgers, which are multi-organizational systems with a robust independent audit that are paired with process characteristics and sensors to form Smart Ledgers. People and organizations are using smart ledgers to manage their identity, payments, obligations, and agreements. A blockchain is used to store immutable, sequenced records in the block, as well as a state database, is used to maintain track of the current state [29].

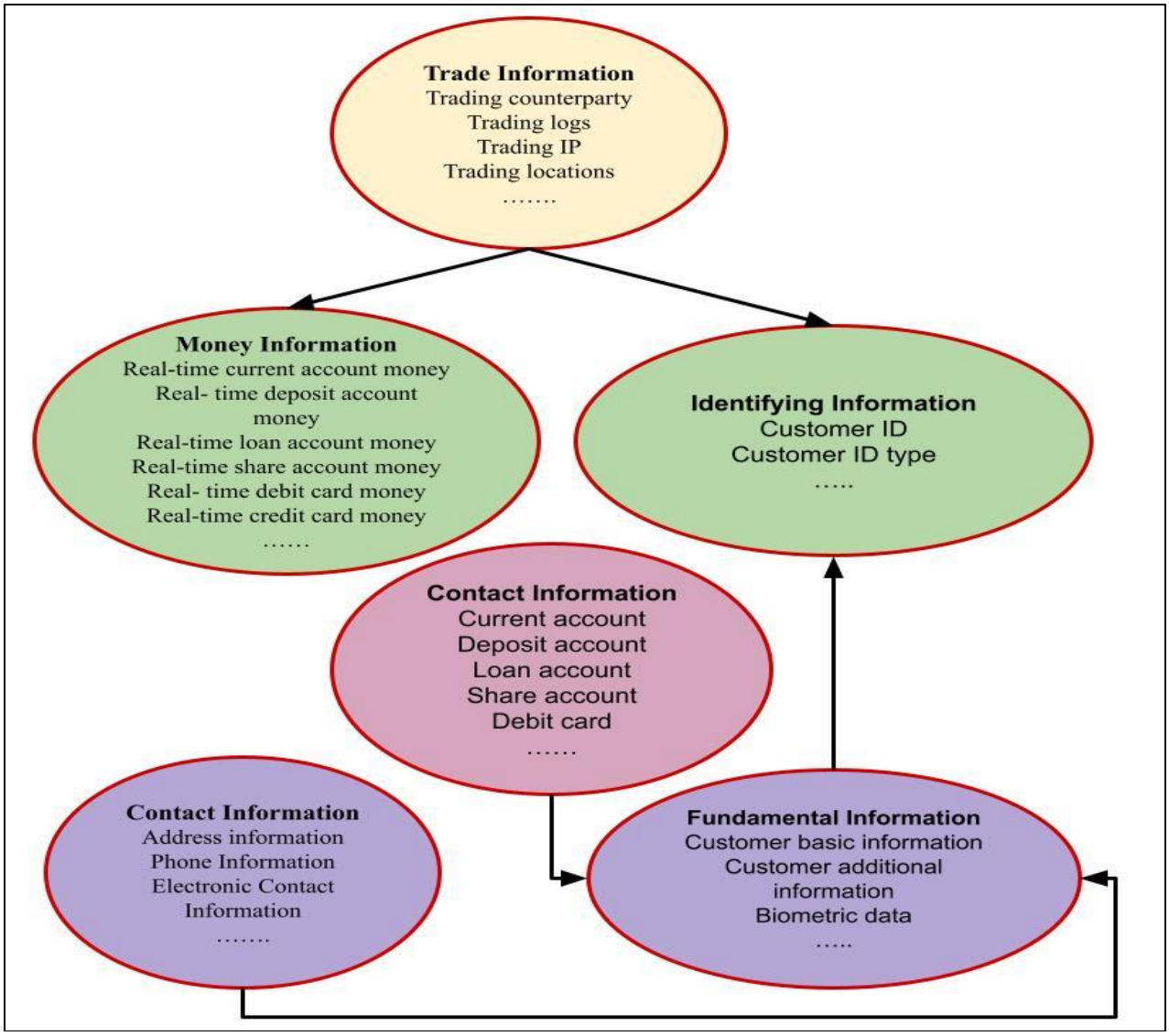
3. Data Security Management Framework Model for Banks with Blockchain Technology

The developed model uses the homomorphic security model framework with the Nudge model for a technical prototype of data management. The conversion of data to a cipher text that can be analyzed and worked upon as if it were that is still in the original form is known as homomorphic encryption. Complicated mathematical operations can be performed on encrypted files without breaking the protection using elliptic curve encryptions. The technique of converting plain text data into something that appears random and pointless is known as encryption. The process of converting cipher text to plaintext is known as decryption [30].

3.1. Characteristics of Financial Data

The customers of banks are categorized as individual and cooperative bank customers. The bank collects data from the customer for financial business for utilization of banking purposes, anti-fraud control, and recommendation of the products. The customer data about financial data reflects the attributes of the customer's financial performance including the transaction of the capital structure and portrait customer information. In Figure 1 the characteristics of the banks and customers in the different aspects are presented based on the customer data entity.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124



Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

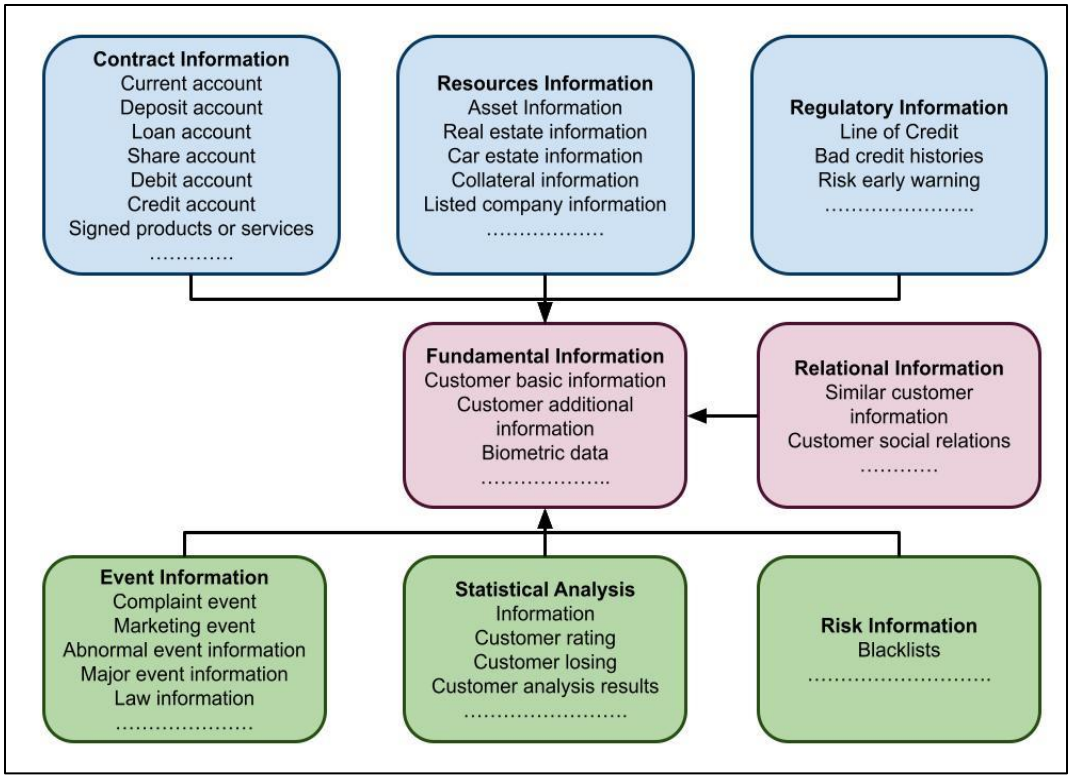


Figure 1.
Entry Point to customer.

The data privacy of the financial data needs to be provided with appropriate priority including the identity of the customers, network data, biometric data, and ethnic data. The basic information is ID number, address, name, and so on. The network data are IP address, RFID, location, and data cookie. The RFID reader is a network-connected gadget that could be either compact or repaired. It transmits signals that trigger the tag through radio waves. Whenever the tag is turned on, it emits a wave back to the antenna, which is converted into data. The Tag contains the transponder. The read range of RFID tags differs determined by some factors, including the kind of tag, reader, RFID wavelength, and disturbance from the environment or other RFID tags and readers. Finally, biometric data are in the form of fingerprints iris, and so on. Biometric data, like facial images or fingerprint data, are personal data resulting from specific technical processing relating to the physical, physiologic, or behavioral features of a normal individual, which enables or confirms the unique identifier of that natural person. To ensure compliance with civil rights legislation and detect indications of bias, routine monitoring of access, use of services, and key processes and outcomes of care by ethnicity and race is essential. Data management privacy needs to provide appropriate rights for the subject data for processing to clarify the use of banking institutions and deal with where and how data. In Figure 2 data privacy model for blockchain technology in banks is presented.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

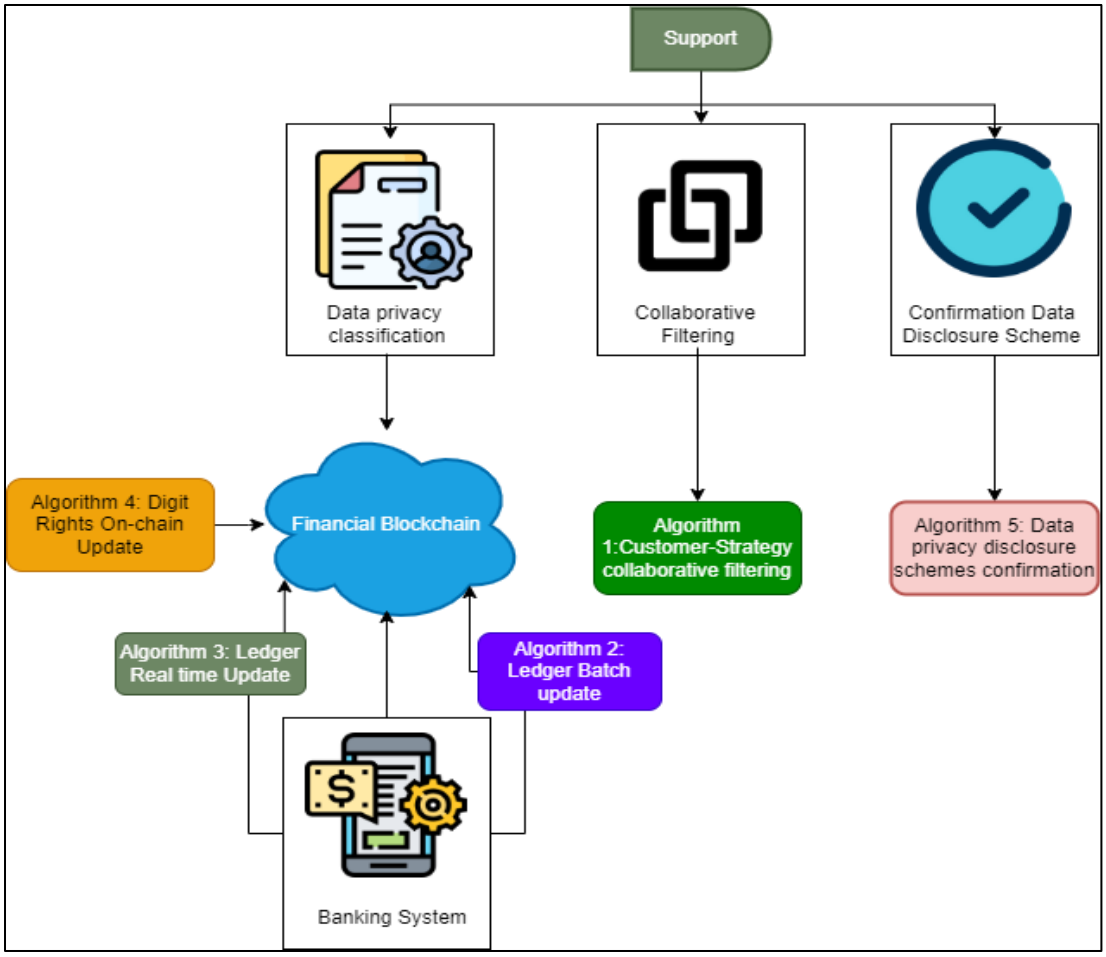


Figure 2.
Data Privacy Model for Blockchain.

The data privacy management framework model comprises three aspects of the processing:

At first, the data privacy management was implemented with the 'Privacy by Design' model for banks to access minimal necessary data for handling the financial data for business through assessment of personal data through appropriate personnel. Privacy by design is a concept that states that organizations should address privacy concerns from the beginning when designing computational practices, rather than adding new features later. Active instead of reactive measures characterize the Privacy by Design (PbD) approach. It envisions and prevents violations of privacy when they occur. It is necessary for effective management of banking data for classification with consideration of different customer dimensions information and provides regulators of customers that facilitate the faster inquiry and monitoring and retention in the characteristics of the blockchain technology. Secondly, with the implementation of a customer data disclosure scheme technologies and algorithms need to be grouped and reduce the signing of artificial contracts. Finally, with the realization of the data dynamic procedure blockchain chain-off will be implemented, enabling periodic updates, customer information addition, and removal.

The bank blockchain technology framework comprises three components such as characteristics of financial data privacy through significant classification methods, construction of the collaborative filtering model, and confirmation of data disclosure and customer strategies with Nudge Theory. Nudge's concept describes positive reinforcement and indirect recommendations as techniques to

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

influence the behavior and decision-making of groups or individuals in behavioral economics, political theory, and cognitive science. Little suggestions and affirmations, according to Nudge theory, may affect customer behavior. Nudge theory argues that the well 'nudges' can help prevent market distortion, save the government money, promote desired behaviors, and optimize resource efficiency. The bank data privacy classification is a basic framework model for classification and disclosure scheme for customer data and collaborative filtering-based model and nudges theory. Machine learning-based bank forecasting allows companies to manage track of entering transaction parameters in real-time. To determine how likely data tends to be fraudulent, the algorithm examines the time series, analyzes customer behaviors, and analyzes other factors.

3.2. Prototype-based on Data Privacy Management

Initially, to secure the bank data homomorphic-based security scheme is developed and implemented. The constructed homomorphic framework model comprises the blockchain-oriented data flow model and liquidation of the interbank network-oriented capital flow model. The banking network is involved in the conversion of the digital rights at the same instance time of the money market that comprises the customer data either on or off in real-time data processing through batch methods shared between banks as illustrated in Figure 3.

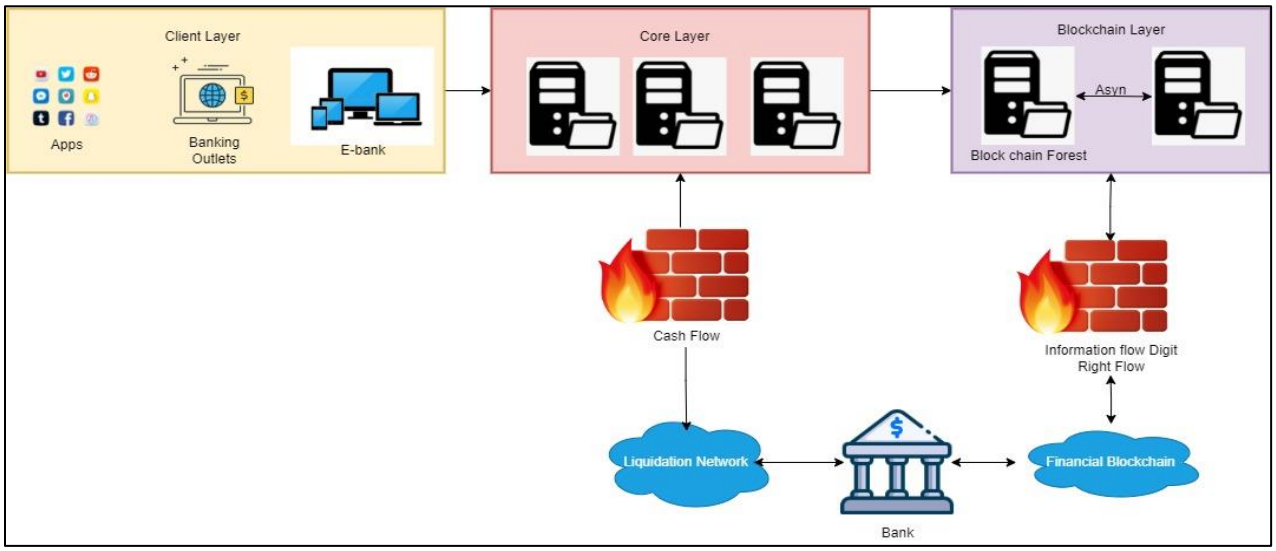


Figure 3.
Characteristics of Nudge Security Model.

3.3. Nudge Collaborative Filtering for Blockchain Technology

The developed blockchain-based secure framework model for banks uses Nudge theory to minimize manual operation and transformation of the system [31]. The nudge model comprises any aspects with overall architecture without modification in the characteristics of people in a predictable manner without affecting options and forbidding economic incentives [32]. The proposed homomorphic nudge theory comprises the disclosure scheme with customer strategy with a collaborative filtering model embedded with the banking process scheme. The data privacy tendency is evaluated in customers of the banks with implicit of the data privacy scheme through collaborative filtering algorithm to calculate the disclosure scheme for new customers and nudge customers in the initial decision. The developed homomorphic data security scheme with nudge theory comprises the customer age, education, industry, position, income attributes, age, financial terms debit card preferences, spending preferences, customer loan, credit card potential, potential debit card, forex customer, transaction high frequency, loyalty of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

the customers and preference for investment. The implementation of the blockchain in banks comprises the privacy management scheme with the implementation of the smart ledger, contract, and data chain on and off.

A customer's smart ledger includes customer information, digital rights, customer data disclosure schemes, and customer information usage situations with equation (1) – (3)

$$\text{Precision} = \frac{|\cap(S_{\text{prediction}}, S_{\text{reference}})|}{|S_{\text{prediction}}|} \quad (1)$$

$$\text{Re } cal1 = \frac{|\cap(S_{\text{prediction}}, S_{\text{reference}})|}{|S_{\text{reference}}|} \quad (2)$$

$$\text{Improved Precision} = \frac{\left|\cap_{\text{inSet}\,(p_1 \sim p_t)}(S_{\text{prediction}}, S_{\text{reference}})\right|}{|S_{\text{prediction}}|} \quad (3)$$

U Cus: the dataset of each bank based on its own dataset information.

$\text{Cus}_j \in \cup\,\text{Cus}$: each customer belonging to the datasets.

$E = \{e_1, e_2, \ldots, e_n\}$:customer information, which e_{ij} represents the j-th subset in the i-th data type;

$R = \{r_1, r_2, \ldots, r_n\}$:digital rights.

$P = \{p_1, p_2, \ldots, p_n\}$:privacy policies.

C: customer-strategy collaborative filtering model attributes of the customers.

$D = \{d_1, d_2, \ldots, d_n\}, d_i = \{p_t \mid e_{ij}\}$ attributes related to customer-strategy

$T =$: confirmation operation in nudging corresponds to e_i.

$U = \{u_{e_1}, u_{e_2}, \ldots, u_{e_n}\}$: the utilization of customer information by the banks.

$L = \{E$、R、 S、U$\}$: blockchain smart ledger.

Tr: transaction triggered by the banking business flow.

Neighbor (Cus $_{\text{new}}$) = (Cus $_{\text{new}\,j}$, Sim (Cus $_{\text{new}}$, Cus $_j$) is Top 5}

The computation is presented in equation (4) and (5)

$$SIM = \cup Sim(CuS_i, CuS_j) \quad (4)$$

$$\text{Neighbor } (\text{Cus}_i) = \{\text{Cus}_j, \text{Sim}(\text{Cus}_i, \text{Cus}_j) \text{is Top } 5\}.$$

$$d_i = p_i\left(\frac{\sum_{\text{Neighbor (Cus } new)}\left(p_t \middle| e_{ij} \in E_{cus_{new_j}}\right) * Sim(cus_{new}, E_{cus_{new_j}})}{\sum_{\text{Neighbor (Cus } new)} Sim(cus_{new}, E_{cus_{new_j}})}\right) \quad (5)$$

In the above equation (5) the term R is represented as a currency of the blockchain based on the application of the specific scenario. The process additionally comprises the information of the customers and applications. The situation of the information usage by the customer is represented as U based on the data for disclosure for the application system and customer data. The smart ledger to the customer architecture model is presented in the figure 4. Figure 4 represents the customer ledger policies, here the smart ledger contains the customer information used for disclosure schemes based on trading.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

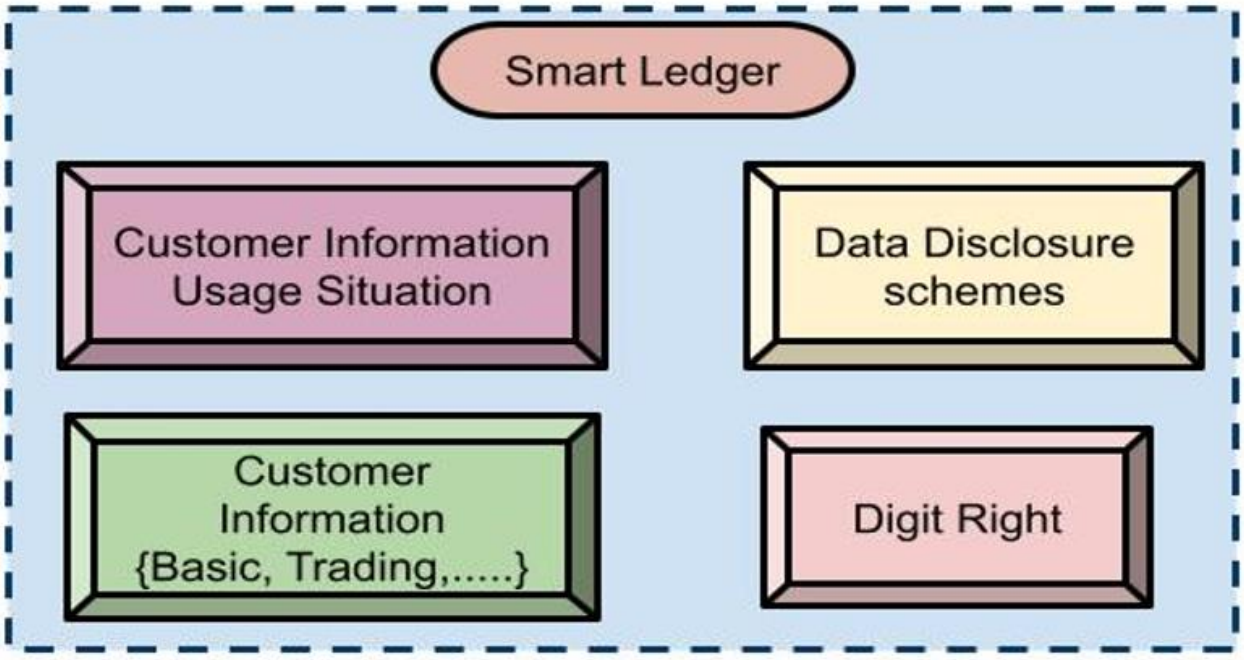


Figure 4.
Customer Ledger Policies.

The algorithm to implement the security framework model for the bank blockchain process is presented as follows:

Algorithm: Homomorphic Nudge Model for Security Framework
Input: Information about customers
Output: Secure model in blocks

1. Check M == Null, proceed step 2
2. Compute the scores for each customer with collaborative filtering
3. Compute the similarity set through cosine function
4. Estimate the nearest neighbour value of the nodes
5. Construct each set for the customers
6. Compute the collaborative filtering through nearest neighbours
7. Calculate

8.

$$d_i = p_i\left(\frac{\sum_{\text{Neighbor (Cus } new)}\left(\left(p_t \middle| e_{ij} \in E_{cus_{new_j}}\right) * Sim(cus_{new}, E_{cus_{new_j}}\right)}{\sum_{\text{Neighbor (Cus } new)} Sim(cus_{new}, E_{cus_{new_j}})}\right)$$

9. Compute the disclosure information of the customers in the banks
10. Update for the non-disclosure customers
11. Compute the nearby blockchain
12. Estimate the encrypted proprietary scheme
13. Update and the consensus confirmation mechanism for customers
14. Schedule each task in the batch and update to ledger
15. Compute the authorized disclosure for the decrypted data for private key extraction
16. Check for the transaction
17. Refresh corresponding electronic and banking account

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

18. Consensus confirmation by the banks to the customers
19. Customer disclosure for e-banks services directly.

4. Experiments

The performance of the developed model is validated with the constructed security framework model. The field analysis and experiments are conducted with the statistical analysis of the customer financial characteristics based on protection of data to verify the usability and strategy of customers with a collaborative filtering model. The experiments are based on evaluation of the security model for the recommended system with security of the blockchain throughput and security.

4.1. Field Experiments

The analysis is based on consideration of the loan details of the customer along with the information based on the disclosure values. The data for analysis is collected from loan customers with a sample count of 1000 who are randomly selected for effective banking services. Among the 1000 customers loan business details are identified and managed through the valid response curve. Figure 5 presents the response plot for the selected data sample was presented. The presented Figure 5 is based on consideration of the disclosure information with consideration of the disclosure information denoted as N.

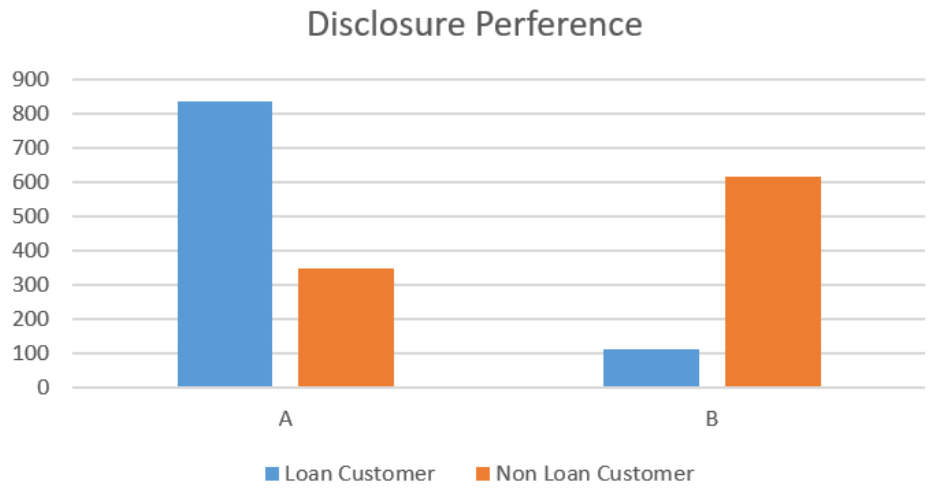


Figure 5.
Distribution of Data Based on Disclosure.

In Figure 5 it is observed that disclosure information agree is denoted as A and disagree with disclosure information is represented as B. The analysis of results expressed that the majority of customers are engaged in loans that are likely with the disclosure information. Also, it is estimated that customers who are young age and have higher educational qualification levels are actively engaged in disclosure information. The customer age is classified into four categories such as 20-30 years, 30 – 40 years, 40 – 50 years and over 50 years. The estimated ratio is in the range of 1:2:2: 3:2. Through stratified sampling technique the people in each category of age are based on customer interview, understanding and communication with disclosure of the banking services with personal information. Sampling is highly beneficial. It's among the most important factors in deciding how reliable your research/survey findings are. If there is indeed a problem with your test, it will be noted in the final result. The various types of sampling techniques are random sampling, stratified sampling, and cluster sampling. Secondly, the educational qualification of the customers in the banks is grouped under 5 categories such as junior school, high school, undergraduate, master, and doctorate. The estimated ratio

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

of the customers is 1:2:9: 6:2. In figure 6 and Figure 7 presented the collected information about the age and education of the bank customers.

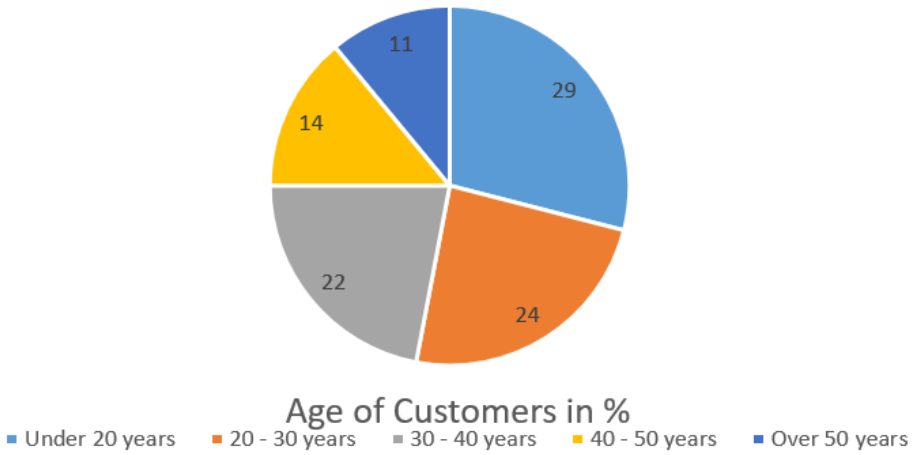


Figure 6.
Distribution of Age of Customers.

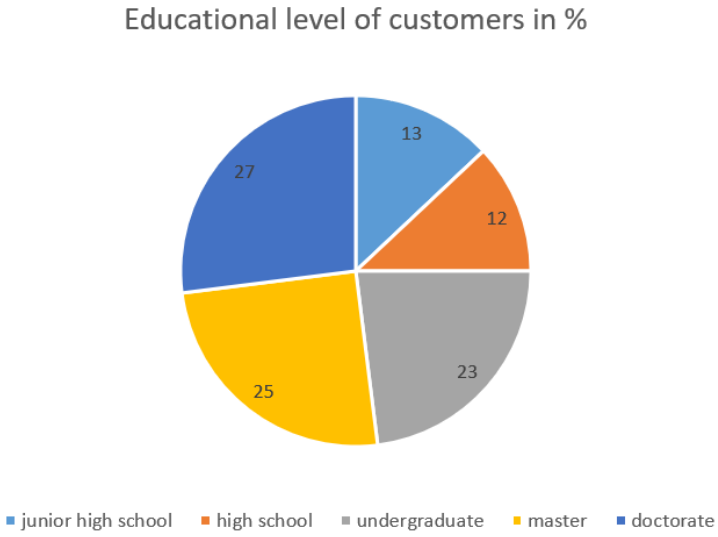


Figure 7.
Distribution of Education Level of Customers.

It is estimated that the customers' age and educational qualification are more likely to agree with the information disclosure in the banks. The data privacy scheme with the Nudge-based collaborative filtering concept is examined for analysis. The experimental analysis is performed with the bank customers concerning bank environment and data disclosure scheme. The dataset considered for analysis is 20000 with attributes of 100 those are identified with the determined policies and records with a data item of 450. The ratio of the training and testing set validation is 4:1 with an estimation of precision, improved precision, and recall. In Table 1 model performance and its results are presented.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

Table 1.
Results for Security Models.

Parameters	Measured Values
Precision	82%
Improved Precision	99%
Recall	23%

The experimental analysis exhibited that the estimated precision is significantly high and the scheme is calculated appropriately. However, the estimated recall is significantly low with the guaranteed data policy and security for the customer data with the nudging operation in the homomorphic scheme for improved security. In Figure 8 under different scenarios, the estimated throughput for the blockchain under different scenarios and nodes in the PC is presented along with the quad-core CPU with the 8 GB memory operation with the transaction per second (TPS) as performance metrics. The number of simultaneous operations performed by a certain person every minute is known as transactions per second (TPS). The volume of transactions per second refers to how often transactions a network can handle per second. The Bitcoin blockchain's median TPS is around 5 albeit this changes from time to time. It is estimated that the higher TPS has the significant blockchain capability those need for data on and off-chain. The average transaction for the bank transaction is estimated as 1000 per second. Hence, the developed model performs effectively in the banking scenario. In Figure 8 estimated TPS for varying numbers of nodes are presented.

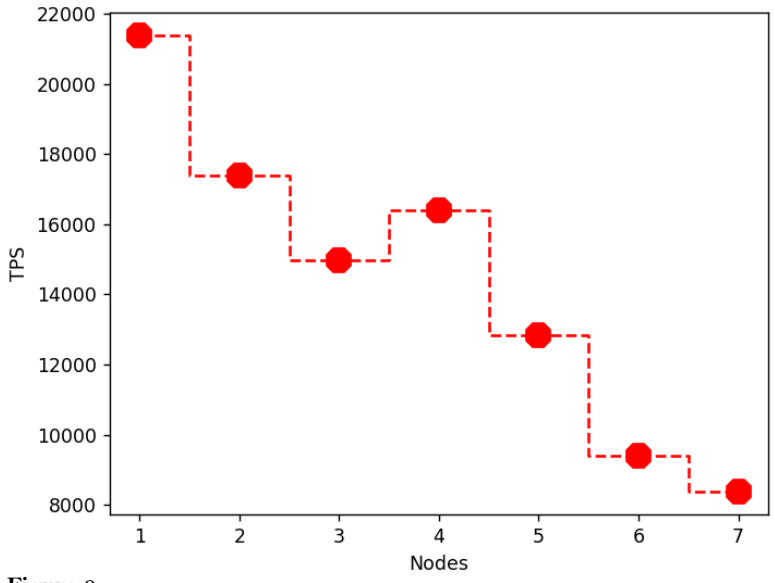


Figure 8.
Estimation of the TPS.

The estimated fault tolerance is computed for the blockchain system with different experimental iterations. Fault tolerance relates to a company's ability to keep on running even if a tiny portion of its hardware and/or software fails. As a consequence, the system designer's goal is to ensure that the risk of system crashes is as low as possible. In the experimental analysis four nodes varying numbers of nodes are engaged for computation of the performance of the blockchain security scheme. The legal transfer for transactions in the banking system exhibits a normal process. In the software environment. The steps in the blockchain security are listed as follows:

1. Create an account for blockchain security and request for permission operation in the account
2. Use the account to conduct the query operation in the successful operation.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

3. Compute the permission query in the null account
4. Utilize the account to operate the query

The permission query fails without any permission in which private information is encrypted and tested with the blockchain information is presented as follows:

1. Create an account for blockchain
2. With open SSL private data is encrypted.
3. View and estimate the cipher text of the data
4. With open SSL cipher text will be decrypted

The operation is implemented prior to the computation of the original data decryption.

Figure 9.
Encryption and Decryption in Blockchain.

With the estimation of the blockchain based cryptography process data were encrypted and decrypted for the security purpose. The estimation is based on the consideration of data authentication and verification. The analysis expressed that the proposed scheme is effective for processing the information of the users in the secure model.

5. Conclusion

In open banking customer data privacy management is considered an important component. However, based on the customer rights and profile of customers is challenging due to security concerns. In this paper developed a data privacy management scheme in blockchain framework management framework with consideration of bank characteristics. The proposed scheme consists of the homomorphic-based customer strategy model integrated with the collaborative filtering algorithm integrated with the Nudge theory for data disclosure. The implemented blockchain model exhibits a data privacy management scheme for financial data scheme. The experimental analysis of the proposed security model exhibits superior performance in banking data privacy. In the future, the proposed security scheme can be tested and validated with different banking scheme models such as loan management and engineering technologies. Additionally, financial blockchain is involved in deletion of the data of the customers in a database of third parties.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

References

[1] H. Hassani, X. Huang, and E. Silva, "Banking with blockchain-ed big data," *Journal of Management Analytics*, vol. 5, no. 4, pp. 256-275, 2018. https://doi.org/10.1080/23270012.2018.1528900

[2] R. Arjun and K. Suprabha, "Innovation and challenges of blockchain in banking: A scientometric view," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 3, pp. 7-14, 2020. https://doi.org/10.9781/ijimai.2020.03.004

[3] N. Cucari, V. Lagasio, G. Lia, and C. Torriero, "The impact of blockchain in banking processes: The Interbank Spunta case study," *Technology Analysis & Strategic Management*, vol. 34, no. 2, pp. 138-150, 2022. https://doi.org/10.1080/09537325.2021.1891217

[4] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, and V. Weerakkody, "Blockchain for next generation services in banking and finance: Cost, benefit, risk and opportunity analysis," *Journal of Enterprise Information Management*, vol. 34, no. 3, pp. 884-899, 2021. https://doi.org/10.1108/JEIM-02-2020-0044

[5] V. Rajnak and T. Puschmann, "The impact of blockchain on business models in banking," *Information Systems and e-Business Management*, vol. 19, no. 3, pp. 809-861, 2021. https://doi.org/10.1007/s10257-020-00468-2

[6] P. Martino, "Blockchain technology: Challenges and opportunities for banks," *International Journal of Financial Innovation in Banking*, vol. 2, no. 4, pp. 314-333, 2019. https://doi.org/10.1504/IJFIB.2019.104535

[7] F. Khanboubi, A. Boulmakoul, and M. Tabaa, "Impact of digital trends using IoT on banking processes," *Procedia Computer Science*, vol. 151, pp. 77-84, 2019. https://doi.org/10.1016/j.procs.2019.04.014

[8] P. Martino, *Blockchain technology and the banking industry. In Blockchain and Banking*. Cham: Palgrave Pivot, 2021.

[9] C. Christodoulou-Volos, "Determinants of non-performing loans in cyprus: An Empirical analysis of macroeconomic and borrower-specific factors," *International Journal of Economics and Financial Issues*, vol. 15, no. 1, pp. 190-201, 2025.

[10] Z. Xie, X. Zhang, and X. Liu, "Enhanced efficiency and security in cross-chain transmission of blockchain internet of ports through multi-feature-based joint learning," *Scientific Reports*, vol. 15, no. 1, pp. 1-17, 2025.

[11] R. Vijay Anand *et al.*, "Design of an improved model using federated learning and LSTM autoencoders for secure and transparent blockchain network transactions," *Scientific Reports*, vol. 15, no. 1, pp. 1-18, 2025. https://doi.org/10.1038/s41598-024-83564-4

[12] Vinayachandra. and P. K. Krishna, "Blockchain-based cryptographic algorithm for data protection in electronic voting system," *EAI Endorsed Trans IoT*, vol. 11, no. 1, 2025. https://doi.org/10.4108/eetiot.7680

[13] H. Liu *et al.*, "Blockchain-based optimization of operation and trading among multiple microgrids considering market fairness," *International Journal of Electrical Power & Energy Systems*, vol. 166, p. 110523, 2025.

[14] S. Kodadi, "Integrating blockchain with database management systems for secure accounting in the financial and banking sectors," *Journal of Science & Technology*, vol. 8, no. 9, pp. 9-27, 2023.

[15] P. Vernekar, P. Anushree, A. K. Chowdhury, and S. Bhoomika, "Implementation of blockchain in the banking sector," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 9, no. 6, pp. 261-265, 2022. https://doi.org/10.32628/IJSRSET229637

[16] I. Hasan and M. M. Habib, "Use of mobile banking, digital payment systems, and smart contracts conjunction with blockchain-based financial system," *International Supply Chain Technology Journal*, vol. 8, no. 11, pp. 1-3, 2022. https://doi.org/10.20545/isctj.v08.i11.0211

[17] X. Xue, "Design of enterprise financial information fusion sharing system based on blockchain technology," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, pp. 1-12, 2022. https://doi.org/10.1155/2022/5402444

[18] H. Wang, S. Ma, H.-N. Dai, M. Imran, and T. Wang, "Blockchain-based data privacy management with nudge theory in open banking," *Future Generation Computer Systems*, vol. 110, pp. 812-823, 2020. https://doi.org/10.1016/j.future.2019.09.10

[19] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," *Internet of Things*, vol. 8, p. 100107, 2019. https://doi.org/10.1016/j.iot.2019.100107

[20] C. DeCusatis, M. Zimmermann, and A. Sager, "Identity-based network security for commercial blockchain services," presented at the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2018.

[21] M. Sumathi and S. Sangeetha, "Blockchain based sensitive attribute storage and access monitoring in banking system," *International Journal of Cloud Applications and Computing*, vol. 10, no. 2, pp. 77-92, 2020. https://doi.org/10.4018/IJCAC.2020040105

[22] P. Garg, B. Gupta, A. K. Chauhan, U. Sivarajah, S. Gupta, and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technological Forecasting and Social Change*, vol. 163, p. 120407, 2021. https://doi.org/10.1016/j.techfore.2020.120407

[23] S. Kamble, A. Gunasekaran, and H. Arha, "Understanding the Blockchain technology adoption in supply chains-Indian context," *International Journal of Production Research*, vol. 57, no. 7, pp. 2009-2033, 2019. https://doi.org/10.1080/00207543.2018.1518610

[24] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," presented at the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2018.

[25] S. Bhardwaj and M. Kaushik, *Blockchain—technology to drive the future. In Smart computing and informatics*. Singapore: Springer, 2018.

[26] P. Raj, K. Saini, and C. Surianarayanan, *Blockchain technology and applications*. United States: CRC Press, 2020.

[27] A. Gupta and S. Gupta, "Blockchain technology application in Indian banking sector," *Delhi Business Review*, vol. 19, no. 2, pp. 75-84, 2018. https://doi.org/10.51768/dbr.v19i2.192201807

[28] W. K. A. Tan and B. Sundarakani, "Assessing Blockchain Technology application for freight booking business: A case study from Technology Acceptance Model perspective," *Journal of Global Operations and Strategic Sourcing*, vol. 14, no. 1, pp. 202-223, 2021.

[29] N. Etaher, G. R. S. Weir, and M. Alazab, "From ZeuS to Zitmo: Trends in banking Malware," presented at the 2015 IEEE Trustcom/BigDataSE/ISPA, 2015.

[30] R. Goyat *et al.*, "Blockchain-based data storage with privacy and authentication in internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14203-14215, 2020. https://doi.org/10.1109/JIOT.2020.3019074

[31] H. Labbadi and A. Khelil, "Blockchain technology application in the UAE banking industry," *Journal of Economics and Finance*, vol. 8, no. 1, pp. 280-294, 2022.

[32] S. N. Wahab, Y. M. Loo, and C. S. Say, "Antecedents of blockchain technology application among Malaysian warehouse industry," *International Journal of Logistics Systems and Management*, vol. 37, no. 3, pp. 427-444, 2020. https://doi.org/10.1108/JGOSS-04-2020-0018

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 1204-1220, 2025
DOI: 10.55214/25768484.v9i5.7124