

BLOCKCHAIN BASED DATABASE SECURITY MECHANISMS IN BANKING CLOUD

Mr. U. Gowrisankar¹, Mr. K. Sudhir², Mr. S. Santhosh³, Mr. S. Vishnuprasath⁴

¹Assistant Professor, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamilnadu, India.

^{2,3,4}Student, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamilnadu, India.

ABSTRACT

Cloud computing provides unlimited infrastructure to store and execute customer data and program. Due to this redundancy the data can be easily modified by unauthorized users which can be stored in the database. This leads to loss of data privacy and security to database. Extensive security and performance analysis shows that the proposed scheme ensures that cyclic redundancy check and time-tested practices and technologies for managing trust relationships in traditional enterprise IT environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc. In addition, blockchain based security mechanism is added in the application. The testing application to enable Data Storage Security in Cloud Computing for Banking Enterprises designed using Microsoft Visual Studio .Net as front end. The coding language used is Visual C# .Net. The web technology used is ASP .Net. MS-SQL Server is used as back end database.

Keywords: Block Chain.

1. INTRODUCTION

It proposes a consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers. It delivers applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. In some cases, legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location. Cloud computing provides unlimited infrastructure to store and execute customer data and program. As customers we do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use.

2. LITERATURE SURVEY

2.1 Blockchain Application for Central Banks: A Systematic Mapping Study

Blockchain is a unique technology that has attracted the attention of Central Banks having enormous disruptive potential. However, it appears that there is a research effort divide between practitioners and academics. This report examines patterns in peer-reviewed research to analyze and map that gap. Contributions made by categorizing scholarly material on Distributed Ledger Technology thematically (DLT) use-cases for central banking services, operations, and functions. Additionally, this paper summarizes the benefits and problems for central banks as a result of blockchain adoption. Each of these use-cases. We employ a Systematic Mapping Study technique to attain this purpose. The report provides an in-depth evaluation of statistical and thematic analyses of research maturity and types of research researchers, with a focus on several forms of central bank. The goal of this mapping project was to look through existing peer-reviewed articles on the impact of blockchain technology on the operations of central banks. The emphasis was on determining what kinds of use-cases existed. were taken into account for blockchain adaptation, according to the research. A discussion on particular use-cases were evaluated, as well as their potential benefits, dangers and issues associated with blockchain adoption. The relevant literature was used to summarize the use-cases. The Systematic Mapping Study discovered a variety of scholarly research has addressed existing blockchain-based use cases for central banks and has offered a complete statistical and Thematic study of various use-cases as

2.2 A Closer Look Into the Characteristics of Fraudulent Card Transaction

The widespread adoption of the Internet, particularly in the last decade, has significantly increased the volume of online card transactions. As online transactions grew, the global banking sector had to grapple with an unexpected surge in fraudulent activities. To address this, rule-based systems were created to flag high-risk transactions and require experts to confirm their fraudulent nature. However, these static rule-based systems were exploited by recent

attacks, allowing fraudulent activities to go undetected. To combat this challenge, researchers began developing adaptive fraud detection systems, primarily utilizing machine learning techniques, including the recent application of deep learning. Their primary focus was on identifying fraudulent activities, but as far as we know, none of them delved into gaining a better understanding of the characteristics of fraudulent card transactions to create more resilient models. In response, our study involved the creation of the most extensive dataset ever used in research, comprising 4 billion non-fraudulent and 245,000 fraudulent transactions contributed by 35 banks in Turkey. Consequently, we introduced and assessed the performance of profile-based fraud detection models, including card-type-based models, transaction characteristics-based models, and amount-based models.

2.3. Improve Profiling Bank Customer's Behavior Using Machine Learning

In the banking industry, the evolution of credit card systems and customer profiling has become increasingly important. Banks collect vast datasets of customer credit card transactions, and customer profiling helps them make informed decisions about whom to offer banking facilities and what credit limits to provide. This profiling is essential for gaining a better understanding of both potential and current customers. Previous research in customer profiling often relied on either transaction data or demographic data, but in this study, the researchers combine both types of data to achieve more accurate results and minimize risks. The study utilizes four different clustering techniques: k-means, improved k-means, fuzzy c-means, and neural networks. These techniques are applied to a labeled dataset, and a new label is created to serve as the target for the neural network classification. This novel approach helps reduce the execution time required for clustering and, more importantly, leads to improved accuracy results. The findings of the study indicate that, after comparing the accuracy ratios of the various techniques, neural networks are identified as the most effective clustering technique for customer profiling in the context of the banking industry.

2.4 Optimal Staffing Policy in Commercial Banks Under Seasonal Demand Variation

Based on both research findings and practical observations, it is evident that the banking sector experiences seasonal variations in customer demand, which significantly impact the operations of commercial banks. Therefore, it becomes imperative for banks to implement a seasonal staffing policy to ensure that their human resources align with the varying customer demands across different seasons. Failure to do so can lead to either a shortage or surplus of staff, thereby adversely affecting the overall efficiency of bank operations. This research paper introduces a novel seasonal staffing approach designed to assist banks in determining the most suitable staffing policy during seasonal fluctuations. To effectively capture the intricacies of bank operations, the study models the service systems of n branches within a bank as n -dimensional M/M/c/N queueing systems, considering factors such as balking (customers refusing to join a queue) and reneging (customers leaving a queue). Subsequently, the research develops a profit-maximizing model based on this queueing system, which is further simplified through linearization, enabling rapid model resolution. Moreover, the research includes a series of numerical experiments aimed at demonstrating the superiority of this new approach over traditional methods.

2.5 Performance, Efficiency, and Target Setting for Bank Branches: Time Series With Automated Machine Learning

Furthermore, the evaluation of bank branches and portfolio managers' performance is based on these quarterly targets. This research primarily focuses on predicting performance using advanced machine learning algorithms. A novel approach is introduced, combining algorithm selection and hyperparameter optimization, to automate machine learning processes for each branch. Since different branches may exhibit distinct customer segmentation and behaviors, this tailored approach is essential. Subsequently, postconditions are applied to finalize target calculations and distribution based on performance predictions. The study demonstrates the effectiveness of this methodology, achieving a remarkable 98% accuracy in performance prediction and the calculation of most branch targets. This end-to-end solution effectively addresses the challenges of seasonality and periodicity that branches often encounter when striving to meet their objectives. Notably, this novel approach enhances the success rate of branch targets by 10% overall. Machine learning techniques are employed to ensure consistency in the analysis of data and to unveil periodic patterns.

2.6 Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis

Biometric authentication is garnering widespread interest across various sectors, including private, public, consumer electronics, and corporate security systems. Organizations, individuals, and enterprises are increasingly turning to biometric security to protect cyberspace from hackers and malicious actors. The term "cybersecurity" encompasses the procedures, techniques, and tools used to safeguard data, network systems, computer networks, and software from potential online attacks. The provision of financial services online is commonly referred to as "cyber banking." The

landscape of internet banking has evolved as a result of changing consumer preferences. However, despite the advantages of online banking, security threats have arisen. Biometric security, which verifies individuals based on their physical attributes and behavioral traits, is considered one of the most reliable and effective methods for identity verification. It allows for precise identification based on these innate characteristics.

2.7 Cyber Threats Classifications and Countermeasures in Banking and Financial Sector

The banking and financial sector has consistently been a prime target for cyber threats because of the sensitive nature of the information they handle. As society increasingly relies on technology and undergoes digital transformation, this sector faces increasingly intricate and sophisticated cyber threats from malicious actors. The banking sector serves as the foundation of a country's economy, intricately connected with various other sectors such as petroleum, mining, healthcare, and industry. Any significant disruption to the banking sector can send shockwaves throughout the entire economic landscape. Consequently, the classification of cyber threats plays a pivotal role in risk management, offering a valuable framework for comprehending and responding to these threats. This research paper's primary objective is to deliver a comprehensive analysis of cyber threats within the banking and financial sectors. This includes identifying common threats, understanding their nature and characteristics for classification purposes. A notable contribution of this research paper is the categorization of cyber threats targeting the banking and financial sectors based on their severity and technical complexity.

2.8 Development of a Customer Churn Model for Banking Industry Based on Hard and Soft Data Fusion

In recent years, there has been a noticeable increase in customer churn, where customers opt not to continue their engagement with an organization's products or services. Customer data can be categorized into two groups: "hard" and "soft" data. "Hard data" encompasses records generated by various devices and software, including but not limited to smartphones, computers, sensors, smart meters, fleet management systems, call detail records (CDRs), and consumer bank transaction data. Conversely, "soft data" refers to information that is open to interpretation and perspective. Integrating these two data types allows for a more comprehensive analysis of customer behavior. This research employs a supervised machine learning algorithm, specifically a decision tree (DT), and change mining techniques to model hard data. Additionally, unsupervised machine learning techniques such as K-means clustering, along with data preprocessing methods, are utilized. The paper also takes into account the Dempster-Shafer theory and other approaches to model soft data. By combining soft and hard data, it becomes possible to calculate and compare customer churn rates.

2.9 Fraud Detection in Banking Data by Machine Learning Techniques

With the advancement of technology and the expansion of e-commerce services, credit cards have gained immense popularity as a payment method, leading to a surge in banking transactions. However, this surge has also brought an increase in fraudulent activities, resulting in higher transaction costs for banks. Detecting and preventing fraud has become a critical area of focus in the financial industry. In this research, we explore the utilization of class weight-tuning hyperparameters to adjust the importance of distinguishing between fraudulent and legitimate transactions. To optimize these hyperparameters while considering the challenges posed by imbalanced data, we employ Bayesian optimization. We introduce weight-tuning as a preprocessing technique for handling unbalanced datasets. Additionally, we incorporate machine learning algorithms like CatBoost and XGBoost to enhance the performance of the LightGBM method by leveraging a voting mechanism.

2.10 A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures

The primary objective of this mapping study was to examine existing academic research papers and conduct a comprehensive statistical and thematic analysis of the use-cases related to the influence of blockchain technology on central banks. This analysis included narrative summaries of the research content for each identified use-case. The study also aimed to establish the overall research maturity by presenting the frequency of publications over time, categorizing papers based on research channels, and demonstrating the depth and breadth of research through various research types, contributions, and cohorts of researchers. One critical point of discussion in this view centered around pinpointing the specific areas and functionalities of central banking that attracted academic interest.

3. EXISTING SYSTEM

These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers to peers. Again, none of these distributed

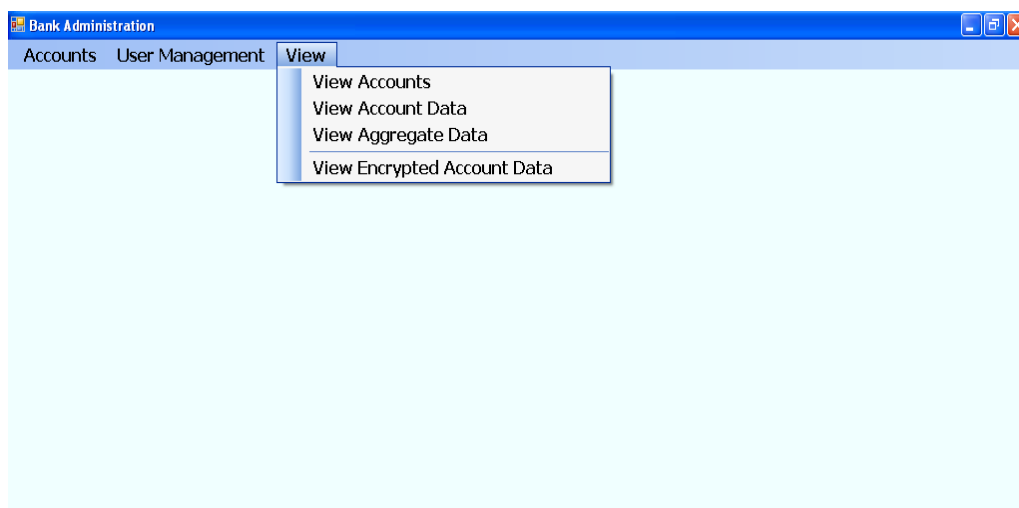
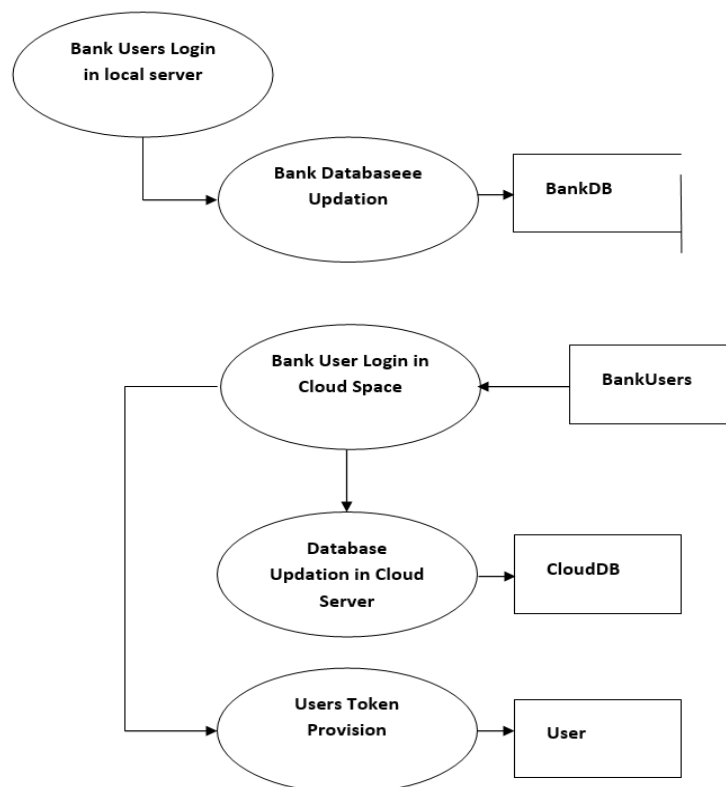
schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited. However, while providing efficient cross server storage verification and data availability insurance, these schemes are all focusing on static or archival data. As a result, their capabilities of handling dynamic data remains unclear, which inevitably limits their full applicability in cloud storage scenarios.

4. PROPOSED SYSTEM

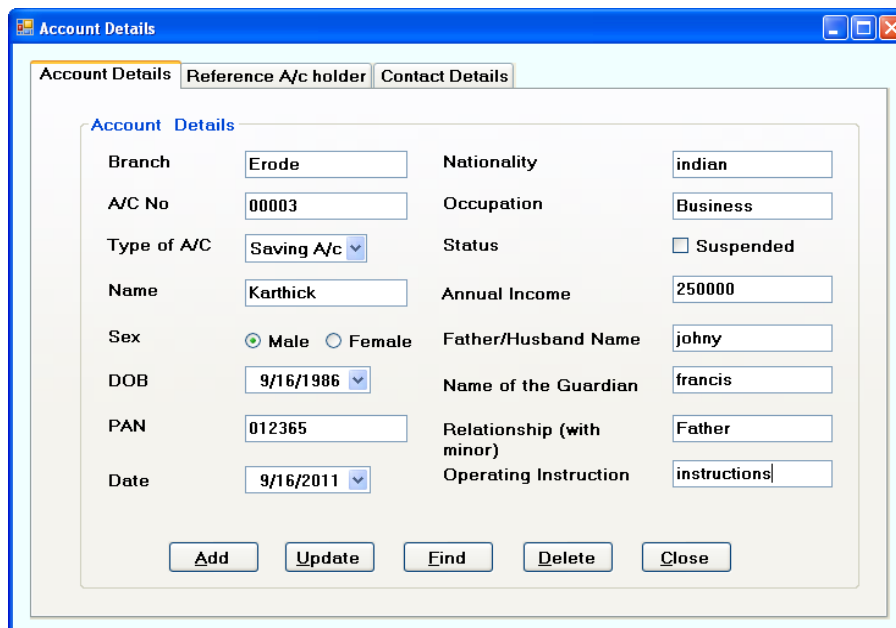
In this project, an effective and flexible distributed scheme is proposed with explicit dynamic data support to ensure the correctness of users' data in the cloud. Some part of the data is encrypted in the cloud storage with a symmetric key encryption. For example, the day to day transaction database records. Their aggregated values are encrypted in data owner storage which is less in size. The database in cloud storage may be redundant and can be accessed by more number of users. To check the data in cloud storage is safe, the sample data can be fetched from cloud storage and decrypted. The aggregated data is also decrypted so that the data from cloud produce the same aggregated data. This ensures the data in the cloud storage is unaffected by users. The storage correctness verification is made in the above manner

5. DESIGN AND IMPLEMENTATION

4.1 DATA FLOW DIAGRAM (BANK USERS MODULE)



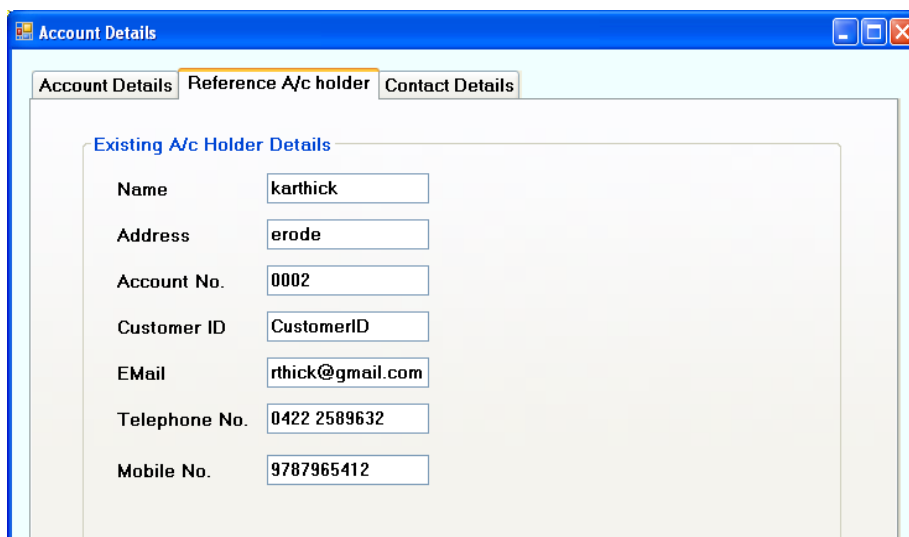
ACCOUNTS:



Account Details		Reference A/c holder		Contact Details	
Branch	Erode	Nationality	indian		
A/C No	00003	Occupation	Business		
Type of A/C	Saving A/c	Status	<input type="checkbox"/> Suspended		
Name	Karthick	Annual Income	250000		
Sex	<input checked="" type="radio"/> Male <input type="radio"/> Female	Father/Husband Name	johny		
DOB	9/16/1986	Name of the Guardian	francis		
PAN	012365	Relationship (with minor)	Father		
Date	9/16/2011	Operating Instruction	instructions		

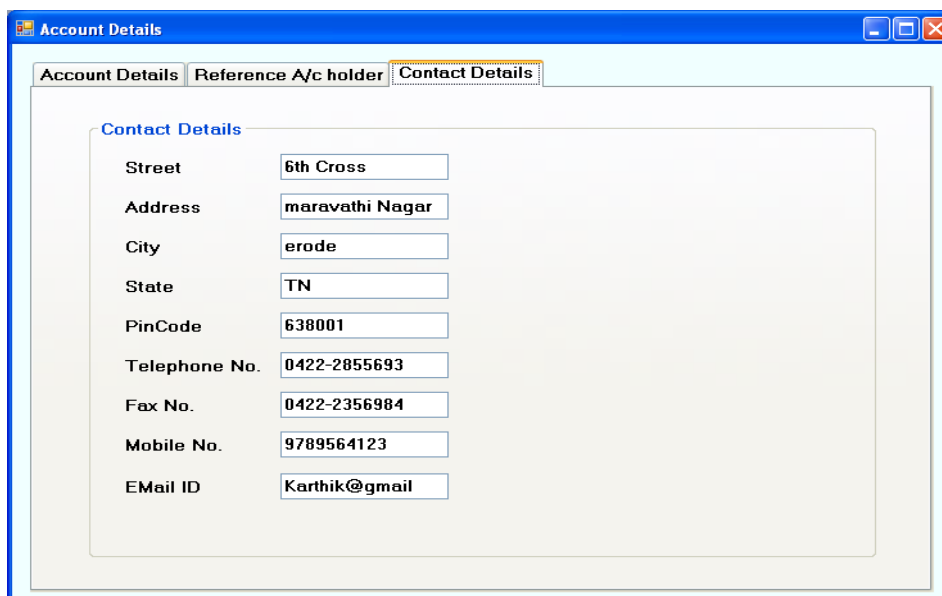
Buttons: Add, Update, Find, Delete, Close

REFERENCE ACCOUNT HOLDER:



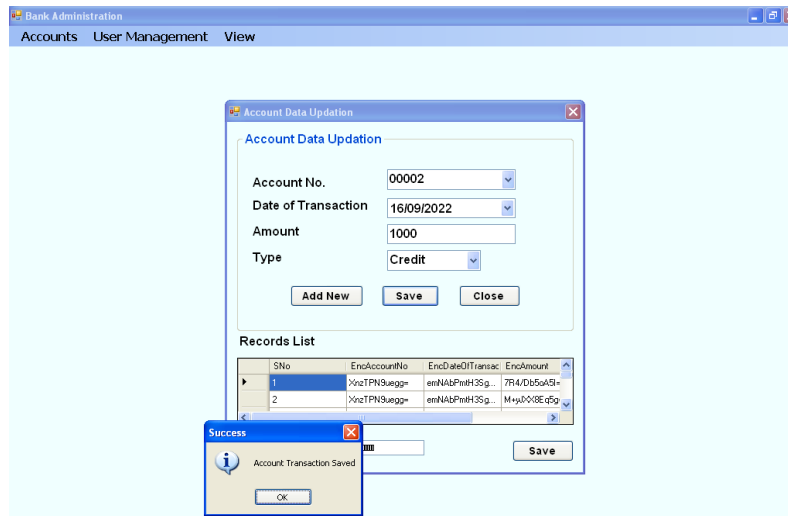
Account Details		Reference A/c holder		Contact Details	
Existing A/c Holder Details					
Name	karthick				
Address	erode				
Account No.	0002				
Customer ID	CustomerID				
EMail	rthick@gmail.com				
Telephone No.	0422 2589632				
Mobile No.	9787965412				

CONTACT DETAILS:



Account Details		Reference A/c holder		Contact Details	
Contact Details					
Street	6th Cross				
Address	maravathi Nagar				
City	erode				
State	TN				
PinCode	638001				
Telephone No.	0422-2855693				
Fax No.	0422-2356984				
Mobile No.	9789564123				
EMail ID	Karthik@gmail				

ACCOUNT DATA UPDATION:



ADMINISTRATOR LOGIN

The administrator logs in to the windows application uses the given username and password using this form. The empty username or password is validated and only after proper username and password is given, the administrator logs in to the application.

ACCOUNTS DETAILS

In this form the accounting details, Reference Id holders, and contact details of the customers (account holders) can be keyed in. The account number being the primary key and is used to enter the transaction details such as credit or debit the account.

ACCOUNT DATA UPDATION

In this form, the data such as account no, date of transaction, amount and type of transaction of accounts can be given. The type of transaction is selected as 'Debit' or 'Credit'. All the values are encrypted and stored in the database.

AGGREGATED DATA UPDATION

In this form, the date of transaction is given, so that the aggregated data is calculated for the given data for both 'Debit' and 'Credit' entries and stored in the database.

ERROR RECOVERY

In this form, the account numbers are populated in a combo box. An account number is selected. Four data grid controls are provided to fetch the records from four databases when 'show data' button is clicked. 'Check For Errors' button is provided to check and display the error records.

USER CREATION

In this form, the UserName and Password is given to create the user. Duplicate username is not allowed since the username field is set as Primary Key (Unique). Empty username or password is not allowed. The various forms used to implement the windows application project concept are

- Home Page
- Login Form

Home Page- In this form, the various login links provided to access the data by the appropriate user, by clicking that particular login

Login Form- In this form, the UserName and Password are keying in the for that particular login and then access the information and also view the particular information.

6. DISCUSSION

This project proposes an model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It proposes a consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers. It delivers applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location.

In some cases, legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location. As customers we do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use. Data can be redundantly store in multiple physical locations. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users now subscribe high quality services from data and software that reside solely on remote data centers. Extensive security and performance analysis shows that the proposed scheme ensures that cyclic redundancy check and time-tested practices and technologies for managing trust relationships in traditional enterprise IT environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc.

7. SCOPE FOR FUTURE DEVELOPMENT

The application become useful if the below enhancements are made in future.

If the application is designed as web service, it can be integrated in many web sites.

The application is developed such that above said enhancements can be integrated with current modules.

8. CONCLUSION

The cloud should take steps to ensure they can trust the companies providing them with services, as well as the entities they are transacting with inside the cloud. Enterprises must have the ability to safeguard proprietary information on virtual servers and storage while giving cloud administrators the access and privileges needed to do their jobs. All of cloud issues relate to establishing trust relationships, which form the conceptual foundations for cloud security. Many of the time-tested practices and technologies for managing trust relationships in traditional enterprise IT environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc. Through this project, the data management process becomes easy. The interface helps bank officials and cloud providers along with customers for accessing the data in the safest way. All the day-to-day activities are assigned to them through browser interface. The new system eliminates the difficulties in the existing system. It is developed in a user-friendly manner. The system is very fast and any transaction can be viewed or retaken at any level. Error messages are given at each level of input of individual stages.

9. REFERENCES

- [1] D. Kim, D. Kwon, L. Park, J. Kim, and S. Cho, "Multiscale LSTMbased deep learning for very-short-term photovoltaic power generation forecasting in smart city energy management," IEEE Mar. 2021
- [2] Alzoubi, H.M., Ghazal, T.M., Hasan, M.K., Alketbi, A., Kamran, R., Al-Dmour, N.A. and Islam, S., 2022, May. Cyber Security Threats on Digital Banking. In 2022 1st International Conference on AI in Cybersecurity. IEEE
- [3] Stanikzai, A.Q. and Shah, M.A., 2021, December. Evaluation of Cyber Security Threats in Banking Systems. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-4). IEEE.
- [4] F. De Arriba-Perez, S. Garcia-Mendez, J. A. Regueiro-Janeiro, and F. J. Gonzalez-Castano, "Detection of financial opportunities in microblogging data with a stacked classification system," IEEE Access, 2020.
- [5] S. Garcia-Mendez, M. Fernandez-Gavilanes, J. Juncal-Martinez, F. J. Gonzalez-Castano, and O. B. Seara, "Identifying banking transaction descriptions via support vector machine short-text classification based on a specialized labelled corpus," IEEE Access, 2020.
- [6] I. Matloob, S. A. Khan, R. Rukaiya, M. A. K. Khattak, and A. Munir, "A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems," IEEE Access, 2022.
- [7] H. Cho, Y. Kim, E. Lee, D. Choi, Y. Lee, and W. Rhee, "Basic enhancement strategies when using Bayesian optimization for hyperparameter tuning of deep neural networks," IEEE Access, 2020.
- [8] A. Arshad, S. Riaz, and L. Jiao, "Semi-supervised deep fuzzy c-mean clustering for imbalanced multi-class classification," IEEE Access, 2019.
- [9] Nicholls, A. Kuppaa, and N.-A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," IEEE Access, 2021.
- [10] D. Caragea, M. Chen, T. Cojoianu, M. Dobri, K. Glandt, and G. Mihaila, "Identifying FinTech innovations using BERT," in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2020.