ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 1, 2018

Leveraging AI and Cloud Computing for Optimizing Healthcare and Banking Systems

[1]Winner Pulakhandam
SIGMA BRIGHT SOLUTIONS INC, Oklahoma, USA
wpulakhandam.rnd@gmail.com

[2]S Bharathidasan
Sree Sakthi Engineering College, Karamadai, Coimbatore
India
sbharathiece@gmail.com

ABSTRACT

This study presents Loan Approval Prediction System-a system that would directly aid in automating decision-making processes in banks. The dataset consists of banking features like credit score, income, loan amount, and various financials of the applicants. Preprocessing procedures, including handling missing values, encoding categorical features, and normalizing numerical data, were done on the data before feeding it into the modeling stage. The model gets trained on distinguishing approved loan applications from rejected loan applications using input data. Then once the model is trained, it will be deployed on the cloud so that it can provide real-time predictions as new applications come in. The classification method used in the system is a feed-forward neural network (FNN), which forwards data through the input layer, hidden layers, and an output layer providing the final loan approval predictions. System performance evaluation yields 98% accuracy, 0.96 precision, 0.94 recall, and 0.95 as the F1 score, thus validating the model's reliability and very strong predictive performance for automating loan decision-making processes.

Keywords: Loan Approval, Feedforward Neural Network, Machine Learning, Cloud Deployment, Data Preprocessing, Classification.

1. INTRODUCTION

Whether businesses or individuals, cloud services have changed the way one manages and stores data [1]. These have become important in the modern computing infrastructure with their scalability, cost- efficiency, and flexibility[2]. However, where dependence on these cloud platforms is growing, so is the need for secure and efficient data protection methods[3]. Although there are numerous security methods available in cloud service providers, the aspects of data protection and privacy still remain a serious concern[4]. They include unauthorized access, data breaches, loss of privacy, etc. The increasing number of threats and the rising volume of sensitive information have increased the requirement for advanced security solutions, particularly those based on artificial intelligence (AI)[5]. AI technologies have the ability to enhance data protection in automating threat detection, risk management, and real-time security monitoring for the confidentiality and integrity of sensitive information[6].

Several factors are believed to be resulting in the increment of demand for AI-based security in cloud services[7]. First of all, the volumes in which data are processed and stored are so enormous that they are far beyond what traditional security systems can handle. Manual monitoring and rule-based systems cannot deal with the magnitude of operations [8]. Hence, they fail to cover security gaps, which arises in such a scenario. Modern cyber-attack schemes are sophisticated, such as phishing, insider threats, and ransomware schemes. These advanced forms of attack demand a better mechanism for detection, learning from previous patterns, and predicting future risks. Also, the evolution of cloud environments continually gives rise to new vulnerabilities and hence the requirements for adaptive intelligence or smart security systems evolve side by side with a threat [9]. Besides, many organizations find themselves legislatively constrained by areas such as GDPR and HIPAA, which necessitate high-level data privacy and protection. Hence, organizations are pushed to adopt such strong, intelligent security enhancing systems.

The benefits that arise with AI-based security solutions also come with disadvantages. One of the most consequential concerns is false positives-the occasional situation when the AI deems legitimate activity to be a threat [10]. This threat can hamper normal business operations and necessitate manual intervention for resolution. AI systems, by their nature, rely on data for training, shortcomings of which may demolish the security models, if the data used is substandard or biased [11]. An additional conundrum is the AI algorithms themselves, some of which are hugely complex and therefore esteeming transparency and acceptance becomes more ambiguous. Organizations may not fully digest the decision-making rationale for AI-based security systems, leading to their

inability to correlate weaknesses and uphold legal and ethical compliance. Also, AI-based solutions tend to demand a lot of computing power, which means smaller organizations or organizations with limited infrastructure might, in general, find them prohibitively expensive.

Given the aforementioned deterrents, organizations could consider adopting a layered strategy in which security systems driven by AI are combined with traditional security tools such as encryption and access control, along with regular audits. Such a hybrid model would allow for a more balanced approach by leveraging AI to detect real-time threats and established security protocols to protect the data [12]. Keeping the AI engine updated with heterogeneous but well-structured data should also act as a lever to improve AI's performance with lower false-positive rates. Explainable AIs (XAI) will serve to increase the security system's transparency and accountability regarding its decision-making process. The support from cybersecurity experts in aligning the AI models with industry standards will help in risk reduction. Optimizing such AI models for scalability and efficiency will ensure significantly less resource burden on organizations and make the most sophisticated security solutions available to a broader spectrum of organizations.

1.1 Contributions

- This paper presents a system for predicting loan approval that is based on machine learning and automates the loan decision process, thus minimizing manual interference while maximizing efficiency in the financial institutions.
- This system is based on the classification of loan applications by employing Feedforward Neural Network (FNN) that shows the prospects of successfully employing deep learning techniques for loan outcomes.
- The trained model is now deployed to the cloud, rendering real-time predictions for loan approval decisions, therefore providing scalability, high availability, and the capability of processing a significant number of loan applications concurrently.
- The model was evaluated in-depth on various classification metrics to prove its usefulness in generating correct loan approval predictions and ensuring minimum misclassification.

2. LITERATURE SURVEY

[13] use ethnography for insights and combine it with big data for analytics to boost healthcare research in cardiology. Some complex interlocks between patient treatment and resource allocation arise; hence, this hybrid approach integrates qualitative ethnography with quantitative data analysis. Things get documented, and trends start getting identified. According to [14] Health Fog is a holistic system where deep learning, IoT devices, and cloud and fog computing work synergistically for rapid diagnosis of infectious and cardiac disorders. Low latency is achieved through processing data from IoT sensors in real-time while using Deep Learning models deployed on the cloud for accurate disease prediction. According to [15] the hybrid AI models and sustainable machine learning being integrated into green logistics aim at reducing the carbon emissions and establishing sustainable supply chains. These are deep learning-optimized algorithm-neural network-options for optimum transport route, vehicle performance, and resource allocation. According to [16] the security framework proposed in this paper improves the security of Cloud-based data using cryptographic algorithms integrated with the secure hash algorithm. It offers data integrity, authenticity, and confidentiality through public-key encryption, digital signatures, and SHA-256 hash values. Furthermore, it provides a robust key management procedure to enhance data transmission, storage, and overall reliability of the system.

According to [17] study spanners for the first time employ Triple Data Encryption Standard (3DES) as an approach for securing data in the cloud environment. This ingestion of three 56-bit keys with special alternating phases of encryption/decryption could provide a better protection than the typical DES. Methodology aspects are: key management protocols; quality improvement through fast key generation and scheduling; and secure storage and delivery systems. Scientific proposals for improving health outcomes for seniors with chronic illness through integrated SDOH, EHR, Multi-Omics Data, and Resource Optimization Models would imply an AI-led framework [18]. Resource optimization hence personalized care is what this framework addresses. It encompasses systemic inefficiencies, such as assuring scalable, affordable, and equitable care for older patients. This study offers a blend of neural fuzzy learning model incorporating fuzzy logic and neural networks for optimistic medical diagnostics through the uncertainty handling of medical data from IoT devices. The model employs machine learning to process real-time data through cloud platforms and to predict normal/abnormal health conditions. The project intends at studying the scalability of real-time production processing data and validating the efficacy of hybrid models for improvement of diagnostic accuracy through IoT-cloud-AI collaboration [19].

Novel avenues have been opened out by graph theory for the comprehension of lung cancer by visualizing biological components as nodes and their links as edges disclosing complex molecular networks. Some prominent techniques applied in this research include structural property analysis, multi-omics integration, predictive

modeling, and therapeutic targets characterization [20]. Classic encryption practices are examined in this research in terms of vulnerabilities, and a hybrid blockchain configuration joining private and public blockchains to enhance information protection implements the results. Moreover, it combines advanced encryption methods such as homomorphic and attribute-based constructions, thus ensuring confidentiality while complemented with intelligent algorithms to address real-time detection of potential threats [21]. Evaluation on the security resilience, encryption efficiency, and latency applied the use of Open Metaverse blockchain datasets. This paper proposes an original framework for integrating IoT devices into cloud-based healthcare systems to address the major issues of scale and inconsistent quality of data. It uses k-Nearest Neighbors for imputing missing values and Z-score normalization for equalizing sensor data management [22].

The research proposes a thoroughly secured document clustering framework that uses Multivariate Quadratic Cryptography (MQC) with Affinity Propagation (AP) to bear upon the confidentiality of data and efficient clustering in IoT scenarios[23]. The framework will resolve the traditional limitation of providing reliable safety, scalability, precision but most importantly scaled up to address performance issues such as computational overhead [24]. This type of next-generation healthcare system will incorporate lightweight CNNs with capsule networks and then some form of DAG-based blockchain to soil the process of increasing diagnostic accuracy and also further scalability to provide decentralization in data security. Use of GANs for synthetic dataset creation for training combining secure data sharing has been used for patching up defects with DAGs while CNNs performed feature extraction and capsule networks spatial representation [25]. This study explored how AI techniques combined with Hierarchical Identity-Based Encryption (HIBE) and Role-Based Access Control (RBAC) provided access controls on the security provision of patient data in mobile health (mHealth) applications. It utilizes Secure Multi-Party Computation (SMC) to support privacy-preserving data processing while optimizing access and security within dynamic mHealth environments. This research deals with addressing security issues in mobile cloud computing by encrypting the data through Diffie-Hellman Key Protocol and using BLAKE2 hashes for fast, secure authentication. Further, the proposed model optimizes efficiency in performance metrics like encryption and decryption speeds and is safe from attack threats toward building mobile cloud computing.

2.1 Problem Statement

Although healthcare information storage and management are fast-paced through cloud computing, it now poses paramount challenges to security and privacy issues regardless of cloud scenarios [26]. Encryption technologies like AES and ECC should ensure secure processing and exchange of data to effectively restrict unauthorized access and data breaches and still comply with the regulatory requirements like HIPAA [27]. Moreover, cloud systems for health services must also contend with the skyrocketing amount and complexity of growing healthcare data and thus would need scalable solutions such as Fog Bus and federated cloud frameworks [28]. These resources should reduce time delays concerning resource access, improve resource management, and provide real-time decision-making in the healthcare environment. Other issues include secure and interoperable identity management systems, for example, Self-Sovereign Identifiers (SSIs), and big data processing in the cloud [29]. The solutions proposed revolve around secure, scalable, and efficient healthcare systems that embody these concerns by using cryptographic algorithms and optimized cloud frameworks towards better data management, resource sharing, and real-time healthcare delivery [30].

3. PROPOSED METHODOLOGY

The primary aim of this is to use machine learning for predicting a loan decision. The first step would be getting the banking dataset with such parameters as credit score, income, loan amount, and the like. The next step would be to prepare the data, which basically involves cleaning a dataset, such as working with missing values and outliers, and normalizing numerical values to optimize modeling. Preprocessed data - this project uses a Feedforward Neural Network (FNN) to classify loans as loan approved or loan not approved. Once trained and evaluated, the model will be deployed on the cloud for real-time loan decision predictions thus automating loan decision-making workflow processes. Thus, the output of the model would be either loan approved or loan not approved

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 1, 2018

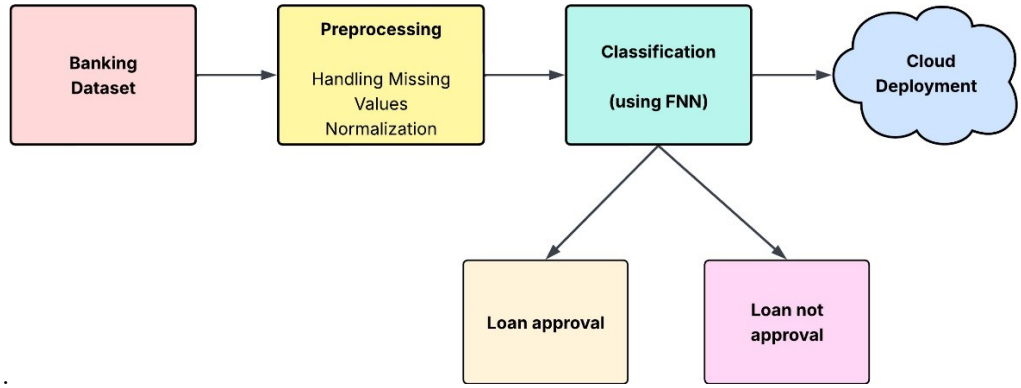

Figure 1: Loan Approval Prediction System Using FNN with Cloud Deployment

3.1 Banking Dataset

The set of data on banks consist of all the structures of the loan applicants. All such applicants and their identities are featured in many applications. The key features would mostly be personal demographic details, such as age, employment status, and marital status, financial information like income, loan amount, and debt-to-income ratio, along with credit history such as credit score, previous defaults, loan purpose, and outcomes of loan applications with regard to whether the loan is approved or denied. These are, in turn, generated to be used in predictive models within credit scoring, prediction of loan approvability, and risk assessments to allow these banks/financial institutions make very sizeable decisions based on data. Hence, this kind of dataset is very relevant for the training of machine learning algorithms that would help in predicting an outcome in a loan and possibly judging default, fraud, or any financial risk.

3.2 Preprocessing

Preprocessing is the most significant phase in machine learning that entails cleaning and transforming the raw data into a model-appropriate format. Missing values are then treated either by imputing with the mean, median, or mode, or by removing incomplete records. These categorical variables are then converted to numerical ones by any one of the encoding techniques, such as one-hot or label encoding. Normalization would make all the input data similar in a given range that enhances model performance. The procedure is also commonly called standardization. Further on identification of outliers from the data, handling might include removal of extreme values or modification to prevent skewing the model. Features engineering may also take place; here the effective generation of new features is done to make the model better predictive. Above all, the preprocessing process makes the data cleaned, consistent, and well-prepared for model fitting.

3.2.1 Handling Missing Values

Handling missing data counts as one of the most significant and important preprocessing stages to be done using machine learning because it distorts the results of the model. Many strategies can help address the complications posed due to the missing attributes, like imputation. Imputation refers to estimating replacement of missing data values by determined values according to existing data. Of course, the most common imputation methods are mean imputation, in which one replaces the missing value with the mean of observed values for that feature. Thus, the feature X can be defined as:

$$X_{\text{imputed}} = \frac{1}{n}\sum_{i=1}^{n} X_i \quad (1)$$

For other non-normally distributed data, median or mode imputation should be applied. When there are large amounts of missing data, advanced techniques, like K-Nearest Neighbors (KNN) or Multiple Imputation, can be used to project the value of the missing ones from observations that are similar.Thus, handling missing values keeps the data sets complete, enabling machine learning algorithms to work well and, thus, prevent bias or inaccuracies in prediction.

3.2.2 Normalization

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 1, 2018

Normalization involves a standardization process by which numerical features are assigned a common effect range. This generally results in values between 0 and 1 so that every feature in the model bears an equal weight, particularly where the different features consume disparate units or have different scales. With an algorithm like gradient-based models, this will be especially important as it will not be sensitive toward this disparity. min-max normalization has been a common technique in normalizing the values of a particular feature x at a certain stated range [0,1] as in the following equation:

$$X_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (2)$$

Where X is the original value, $X_{\min}$ is the minimum value of the feature, $X_{\max}$ is the maximum value of the feature. Transform in this way guarantees that every value of the feature is in the range of [0,1], thus it prevents high scale features from taking control over the learning process and the performance and convergence speed are better than that of many machine learning algorithms.

3.3 Classification (using FNN)

Feedforward Neural Networks (FNNs) perform classification tasks and therefore have to be trained for some predetermined categorizations. Examples of these types of categorizations could be approved or not approved for a loan. The model takes information of the borrower: credit scores, income, amount of loan, and other finances, through the input layer. The input of the model moves into one or more layers, which are regarded as hidden layers. As it moves through these layers, the network learns through the weighted connections and activation functions as to which patterns to develop and how to relate the input features with the output. The output from the last layer (the output layer) is a classification result based on the patterns learned: "loan approval" or "loan not approval." A sigmoid activation function is typically used in the binary case, giving a score from 0 to 1. If this score exceeds a certain threshold, usually set at 0.5, then it predicts approval; otherwise, it predicts non-approval. Trained FNN models can be hosted in a cloud, allowing them to provide real-time predictions for any new loan application and thereby automate the loan decisioning process.

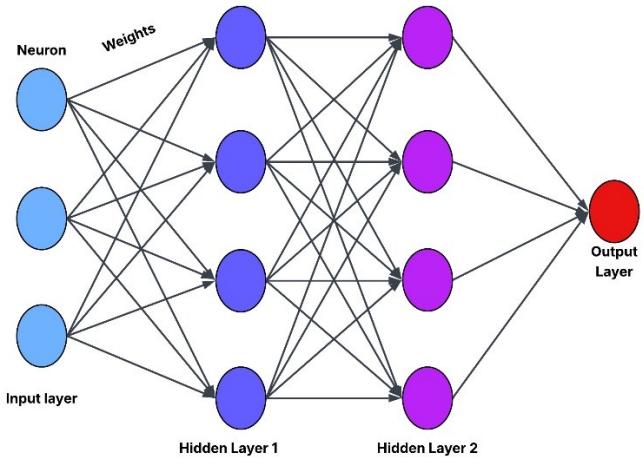

Figure 2: FNN Architecture

3.3.1 Input Layer

The input layer refers to the first layer of a neural network, where raw information is fed into the model. From the parameters of the problem being solved, e.g. credit score, income, loan amount, etc., each neuron of the input layer corresponds to one feature of the data set. The function of the input layer is entirely submissive: it does not do any computations, merely passing the information along to the next layer. If $X = [X_1, X_2, \dots, X_n]$ is the vector of features representing the input data, where $X_1, X_2, \dots, X_n$ are individual features (like age, income, etc.), Input data themselves are simply transferred to the next layer without being altered or transformed in any way. That means, mathematically, there are n features in the input and n neurons in the input layer representing one feature each.

$$X = [X_1, X_2, \dots, X_n] \quad (3)$$

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 1, 2018

Where X is the feature vector that will be passed onto the hidden layers for further computation.

3.3.2 Hidden Layers

Hidden layers play an important role in the learning complex patterns and representation of input data, but each neuron in the hidden layer calculates the weighted sum of the input, adds distortion, and passes this amount to the activation function to introduce nonlinearity. Mathematically, the edition of the hidden layer j-ten neurons is

$$Z_j = \sum_{i=1}^{n} W_{ij} X_i + b_j \quad (4)$$

Where Z_j is the weighted sum for the j-th hidden layer neuron, W_{ij} is the weight between the i-th input feature and the j-th hidden neuron, X_i represents the i-th input feature from the input layer, b_j is the bias term for the j-th neuron. Hidden layers allow the neural network to capture non-linear relationships in the data while helping the model gain insight into more complex features for accurate predictions. Each hidden layer iteratively learns all of the features from the last layer, allowing the model to apply more abstract, higher-level patterns.

3.3.3 Output Layer

The output layer, which serves as the neural network's final layer, is responsible for producing the predictions. Taking input from the previous layer, hidden or otherwise, the output layer computes a weighted sum using that same input plus a bias, applies an activation function, and produces the output in its final form. In classification, the output layer is typically responsible for binary classification using the logistic, or sigmoid, function so that its output can be interpreted as confidence of the model with respect to a class in the range of 0, not belonging to the class, to 1, completely belonging to the class. The formula for the output of the network is as follows:

$$Z_{\text{output}} = \sum_{j=1}^{m} W_j' A_j + b_{\text{output}} \quad (5)$$

Where Z_{output} is the weighted sum of inputs from the last hidden layer, W_j' is the weight between the j-th neuron in the last hidden layer and the output layer, A_j is the output from the j-th neuron in the last hidden layer, b_{output} is the bias term for the output layer.

3.4 Cloud Deployment

Cloud deployment refers to the deployment of a trained machine learning model into the cloud, from where it can be accessed for real-time predictions in a scalable manner. After training the model, in our case, a Feedforward Neural Network (FNN) for predicting loan approvals, it is deployed into a cloud platform, say, AWS, Google Cloud, or Microsoft Azure. The model now handles new loan applications by providing the relevant input features (such as income, credit score, loan amount, etc.) through an API. It makes predictions (loan approval or rejection) and sends the result back to the application. The advantages of cloud deployment include scalability, high availability, easy updates, and the ability to handle many simultaneous incoming requests. It also ensures unrestricted access to the model, which can be conveniently integrated into financial systems for automated decision-making.

4. RESULT AND DISCUSSION

This section on results and discussions was centered around the evaluation of the Loan Approval Prediction Model through various performance metrics. Accuracy gives a measure of how correct a model is in general; on the other hand, precision exemplifies how good a model is in identifying the loan approvals and not misclassifying them as denials. Recall goes toward measuring the ability to identify all loan approvals, and the F1 score attempts to find the balance between precision and recall. All these indicators put together endorse that the model is calibrated and can give credible predictions about loan approvals. We have, however, drawn a further distinction, presenting a confusion matrix specifying the correct classification and misclassification of the model's predictions. It is reasonable to conclude that the model was fairly good, with regard to the higher true-positive and true-negative classifications, in terms of accuracy, having pushed a bit onto a couple of false positives and a couple of false negatives.

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 1, 2018

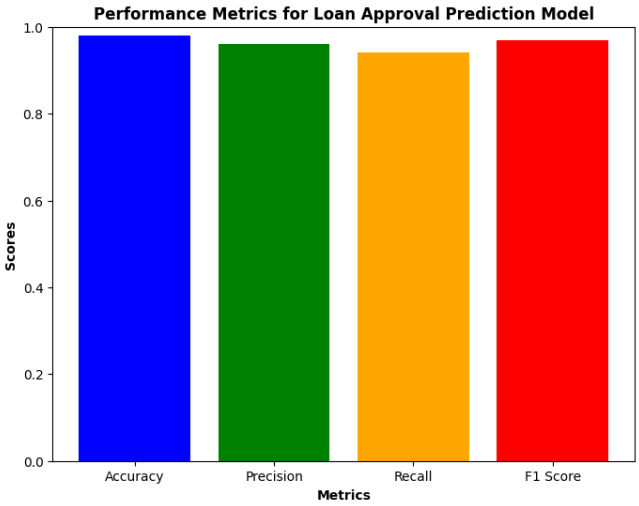

Figure 3: Performance Metrics for Loan Approval Prediction Model

Figure 3 gives performance indicators of the Loan Approval Prediction Model, which presents Accuracy, Precision, Recall, and F1 Score of the model. Each vertical bar indicates one evaluation metric, and each score hovers near 1.0, meaning it is an excellent performance indicator. The blue bar, meaning Accuracy, therefore indicates that most of the time, the model is correct in predicting the outcome for loans.For example, the green Precision indicates to what extent this model identifies approval of loan applications without rendering incorrect decisions to approve denials. Recall, as was portrayed by the orange bar, is about the model's ability to find all loan approvals, including those that could be missed. The F1 Score, in red, goes on to indicate how well the model does, taking into account its ability to identify loan approvals against its differences in misjudging others as loan approval. Very close values of precision, recall, F1, and accuracy suggest that the model is well calibrated to make reliable loan approval predictions.

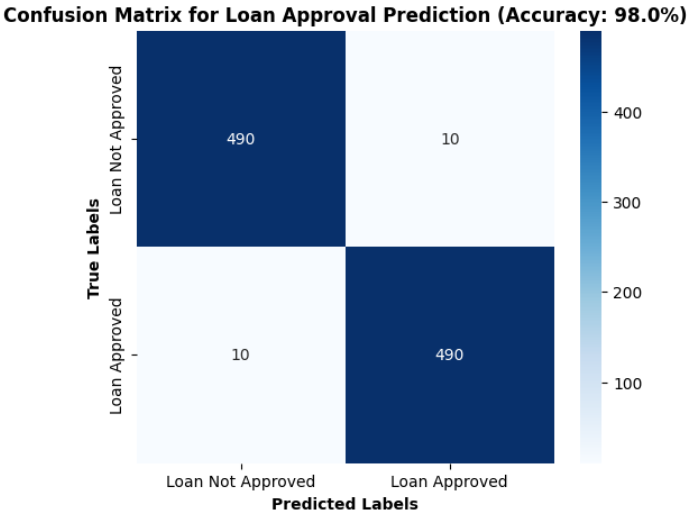

Figure 4: Confusion Matrix

This configuration in Figure 4 shows the confusion matrix for the loan approval prediction model with an accuracy of 98%. True labels (actual loan approval status) compare with predicted labels for the quantification of performance. True negatives at the upper left cell (490) indicate that the model accurately forecasts loans that were actually denied. In the top right cell, the false positives (10) mean the model predicted a loan was granted, whereas it had been rejected in truth. The false negatives (10) that sit in the lower left cell mean that the model predicted that the loan would be denied when it was actually going to be granted. The true positives (490) in the lower right cell indicate that the model accurately predicted the approval of those loans. With an above-average number of right predictions compared to little false predictions, it can be termed as an excellent model for loan forecasting.

5. CONCLUSION

In this study, we designed a Loan Approval Prediction System, which employs machine learning methods to automate the loan decision-making process in the banking sector. The system, based on Feedforward Neural Networks (FNN), showed outstanding predictive ability with 98% accuracy, 0.96 precision, 0.94 recall, and an F1 score of 0.95, indicating efficacious performance in the classification of loan approvals. Being deployed on the cloud, real-time prediction of loan applications has been made possible, making it a scalable alternative for financial institutions and evidently speeding up the decision-making process by using the system. With a very low misclassification rate (unveiled through the confusion matrix), the model stands effective in predicting the loans, approved as well as rejected. This work, therefore, points toward the feasibility of AI systems in rendering much quicker, efficient, and accurate loan approvals in financial services. There is a possibility of improving the performance of the system if it allows for some extensions with very complex features, namely advanced customer demographics or transaction history. Furthermore, improvements of transparency in the decision-making process through the application of explainable AI (XAI) methods will work in favor of greater interpretability of the model, thereby aiding the financial institutions in establishing faith in the predictions of the system.

References

[1] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic, "Smart power grid and cloud computing," *Renewable and Sustainable Energy Reviews*, vol. 24, pp. 566-577, 2013.
[2] M. B. Mollah, K. R. Islam, and S. S. Islam, "Next generation of computing through cloud computing technology," in *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Apr. 2012, pp. 1-6.
[3] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 International Conference on Computer Science and Electronics Engineering*, vol. 1, Mar. 2012, pp. 647-651.
[4] R. Barona and E. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," in *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Apr. 2017, pp. 1-8.
[5] D. S. Terzi, R. Terzi, and S. Sagiroglu, "A survey on security and privacy issues in big data," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec. 2015, pp. 202-207.
[6] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners' attitudes and opinions," in *2013 Information Security for South Africa*, Aug. 2013, pp. 1-8.
[7] M. Cinque, D. Cotroneo, and A. Pecchia, "Event logs for the analysis of software failures: A rule-based approach," *IEEE Transactions on Software Engineering*, vol. 39, no. 6, pp. 806-821, 2012.
[8] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64-71, 2016.
[9] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl, "Stack overflow considered harmful? The impact of copy&paste on android application security," in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 121-136.
[10] I. W. Fung, T. Y. Lo, and K. C. Tung, "Towards a better reliability of risk assessment: Development of a qualitative & quantitative risk evaluation model (Q2REM) for different trades of construction works in Hong Kong," *Accident Analysis & Prevention*, vol. 48, pp. 167-184, 2012.
[11] X. Wang, X. Li, and V. C. Leung, "Artificial intelligence-based techniques for emerging heterogeneous network: State of the arts, opportunities, and challenges," *IEEE Access*, vol. 3, pp. 1379-1391, 2015.
[12] J. S. Rumsfeld, K. E. Joynt, and T. M. Maddox, "Big data analytics to improve cardiovascular care: promise and challenges," *Nature Reviews Cardiology*, vol. 13, no. 6, pp. 350-359, 2016.
[13] D. Zhang, L. Wang, and Z. Yang, "Nature products and cardiovascular disorders," in *Frontiers in Cardiovascular Drug Discovery: Volume 2*, pp. 3-91, Bentham Science Publishers, 2015.
[14] B. Fahimnia, J. Sarkis, A. Choudhary, and A. Eshragh, "Tactical supply chain planning under a carbon tax policy scheme: A case study," *International Journal of Production Economics*, vol. 164, pp. 206-215, 2015.
[15] M. Aledhari, A. Marhoon, A. Hamad, and F. Saeed, "A new cryptography algorithm to protect cloud-based healthcare services," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Jul. 2017, pp. 37-43.
[16] I. Hosni and N. Hamdi, "Identified improvements of wireless sensor networks in smart grid: issues, requirements and challenges," *International Journal of Smart Grid and Green Communications*, vol. 1, no. 1, pp. 3-37, 2016.
[17] D. W. Bates, S. Saria, L. Ohno-Machado, A. Shah, and G. Escobar, "Big data in health care: using analytics to identify and manage high-risk and high-cost patients," *Health Affairs*, vol. 33, no. 7, pp. 1123-1131, 2014.
[18] S. Lazarova-Molnar, H. R. Shaker, and N. Mohamed, "Fault detection and diagnosis for smart buildings: State of the art, trends and challenges," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, Mar. 2016, pp. 1-7.
[19] M. Bersanelli, E. Mosca, D. Remondini, E. Giampieri, C. Sala, G. Castellani, and L. Milanesi, "Methods for the integration of multi-omics data: mathematical aspects," *BMC Bioinformatics*, vol. 17, pp. 167-177, 2016.

[20] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601-628, 2017.
[21] S. V. Patel and V. N. Jokhakar, "A random forest based machine learning approach for mild steel defect diagnosis," in *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Dec. 2016, pp. 1-8.
[22] L. F. da Cruz Nassif and E. R. Hruschka, "Document clustering for forensic analysis: An approach for improving computer inspection," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 46-54, 2012.
[23] Y. Liu, J. E. Fieldsend, and G. Min, "A framework of fog computing: Architecture, challenges, and optimization," *IEEE Access*, vol. 5, pp. 25445-25454, 2017.
[24] S. Majumder, T. Mondal, and M. J. Deen, "Wearable sensors for remote health monitoring," *Sensors*, vol. 17, no. 1, p. 130, 2017.
[25] A. A. Eludire, J. B. Elusade, J. A. Agbakwuru, T. C. Nwaoha, A. A. Adedotun, G. T. Cosmas, ... and S. A. Folorunso, "West African Journal of Industrial & Academic Research," *West African Journal of Industrial & Academic Research*, vol. 15, no. 1, p. 1, 2015.
[26] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431-1441, 2014.
[27] J. Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial internet: A survey on the enabling technologies, applications, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1504-1526, 2017.
[28] J. Torres, M. Nogueira, and G. Pujolle, "A survey on identity management for the future network," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 787-802, 2012.
[29] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678-708, 2015.
[30] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, ... and S. Andreescu, "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges," in *2015 IEEE International Conference on Services Computing*, Jun. 2015, pp. 285-292.