ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 12, Issue 3, 2018

Fraud Detection in Cloud-Based CBS Using CNN

[1]**Bhagath Singh Jayaprakasam**
Cognizant Technology Solutions, Texas, USA
Bhagath.mtech903@gmail.com

[2]**R. Hemnath**
Kaamadhenu Arts and Science College, Sathyamangalam,India.
hemnathrmca@gmail.com

Abstract:

The integration of cloud computing into banking systems has allowed operations to become scalable, effective, and secure, thus completely transforming the financial industry. Conventional banking systems, typically premised upon on-site technology, give way to a number of drawbacks, such as slow transaction processing, high operational costs, and limited avenues for scalability. These shortcomings hinder the adoption of real-time detection technologies for fraud, which are a must to counteract financial loss. In this work, we design a novel cloud-based fraud detection system for real-time fraud detection in a Core Banking System (CBS) based on CNN deployed on AWS Lambda. We create a deep learning model based on multiple features of a transaction that include amount, location, and user behavior, in order to ascertain whether a transaction is fraudulent or legitimate. The model performed an F1 of 93.0%, accuracy of 97.5%, precision of 90.9%, and recall of 95.2% in test results using AWS Glue for configuration and Amazon RDS for storage. Appearing with low latencies and high throughput, the model is considered good in fraud detection. Our work is a more reliable, scalable, inexpensive, and highly efficient method of fraud detection in today's finance systems as compared to the conventional methods.

Keywords: *Fraud Detection, Cloud-Based Core Banking System, Convolutional Neural Network (CNN), AWS Lambda, Real-Time Prediction, Machine Learning*

1.Introduction:

Cloud computing has revolutionized conventional ways of doing banking, as it provides scalable, flexible, and reasonable solutions[1][2]. Banks get it more secure, store data, and process more transactions using cloud-based solutions of finance in real time. [3] [4]. All of these participated in cloud infrastructure and finally led to the innovative services of fraud detection in real time, mobile banking, and tailored experiences for customers. The cloud will allow any financial institution to cut down on operational cost while improving system reliability and agility in the face of changing market demand.[5] [6]. Thus, cloud technology is rapidly becoming an enabler for modern banking and the future of digital transformation within the financial world [7].

Bank fraud detection systems today are mainly rule-based and basic machine learning models, coupled with traditional on-premises infrastructure [8] [9]. These systems are, by their very nature, poorly scalable, expensive to maintain, and not able to handle thousands of transactions in real time. Hence, response time lags due to the processing of the input, which delays the fraud identification [10]. Majority of such systems are hampered by inadequate processing powers and low adaptability, even if some of them use some machine-learning techniques.[11] [12]. These systems are under huge stress in the changing pattern of fraud and real-time data acquisition, as the demand for fraud detection is increasing.[13] [14]. On the other hand, a lack of cloud scalability due to infrastructure being static makes current and flexible fraud detection methods hard to maintain[15] [16].

The modern financial fraud detection systems have limited effectiveness because they solely depend on traditional on-premise infrastructure, leading to non-scalability, costly operational expenses, and no real-time processing. Additionally, these systems are generally unresponsive to changes in fraud trends and are not computationally sufficient to run a huge amount of transactions efficiently. Our methodology overcomes these hurdles through cloud-based infrastructure and Convolutional Neural Networks (CNNs) to implement low-latency, scalable, real-time fraud detection through AWS Lambda. By tapping into cloud-based services such as Amazon RDS for storage and AWS Glue for data processing, our approach is making the systems more responsive and cost-

effective, thus providing a more agile and reliable method of fraud detection. The research enables the creation of a scalable, cost-effective and flexible fraud detection system which can handle large transactional volumes with versatility as to adjusting to newer patterns of fraud over time.

1.1.Problem statement:

As transactions are done instantaneously, online and mobile banking's essentiality has put more and more pressure on core banking systems to detect fraud[17] [18]. Because of limited scalability, very high operating costs, and slow processing time, traditional fraud-detection systems cannot handle enormous transaction data. Most commonly, these systems are based on on-premise infrastructure[19] [20]. As fraud prevention becomes more and more sophisticated, the banking systems need to integrate real-time detection models for identifying fraudulent transactions with little or no delay [21]. Applying serverless architecture with technologies such as AWS Lambda and cloud computing with deep-learning approaches (Convolutional Neural Networks), this study attempts to propose a fraudulent detection solution for cloud-based core banking systems that scales and remains affordable[22] [23]. The proposed scheme targets high latency reduction, increased accuracy of fraud detection, and more flexible response to shifting trends of fraud characteristic in modern-day financial environments[24], [25].

1.2.Objective:

1. Develop a cloud-based fraud detection application using Convolutional Neural Networks (CNN).

2. Ensure real-time fraud detection with low latency using AWS Lambda.

3. Evaluate the effectiveness of the fraud detection system using critical metrics: accuracy, precision, and recall.

4. Optimize scalability and cost-effectiveness of fraud detection through cloud infrastructure.

The rest of the paper is organized as follows. Section 1 with the introduction. Section 2 will discuss the Theoretical Background. Section 3 presents the Methodology and Section 4 highlights the results. Section 5 concludes.

2.Literature review:

Cloud computing, as suggested by Ghule, promotes innovation and enhances the financial service delivery process with agility, considered paramount in the success of any financial organization [26]. Asadi et al., proposed the TAM-DTM model with modifications by introducing trust, cost, and security as additional constructs to look into the factors influencing cloud computing adoption in the banking industry from a consumer perspective[27]. They found that consumers' behavioral intention to use cloud computing is significantly influenced by the perceived usefulness and perceived ease of use, which in turn are positively influenced by trust, cost, and security. In comparisons with the banking industry, wherein security and trust are a matter of primary concern for the clients themselves and also the service providers, Bose et al., discussed the importance of these perspectives in cloud adoption[28]. Apostu et al., studied decision-making processes for cloud adoption in the banking industry, with respect to business problems that would be solved by this implementation of cloud computing[29]. Elzamly et al., showed how performance of ANN can be increased in predicting security levels in the cloud by means of combining ANNs with the Levenberg-Marquardt Back Propagation techniques to predict cloud security levels[30].

Mugyenyi outlined the Ugandan commercial banks expansion efforts encountering challenges due to exorbitant operational costs, demand for IT infrastructure, and inadequate data storage management [31]. The research established that scalable data management and storage capabilities of cloud computing could present a possible solution. Kshetri et al., argued that the developing world needs to harness the benefits of cloud computing while minimizing its dangers in order to have access to modern IT infrastructure and to protect sensitive information[32]. Buyya et al., investigating the capabilities of InterCloud for cloud systems federation, showed an improvement in performance, response time, and cost-effectiveness [33].Cloud computing, according to Aljabre (9), would be the new paradigm of the future in business operations and particularly highlighted the competitive advantages that smaller businesses stand a better chance of enjoying from its application [34]. The final authors to contribute to

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 12, Issue 3, 2018

this growing body of literature on how companies can benefit from cloud computing as Chard et al., on the idea of a "Social Cloud," where social networks would facilitate resource sharing with less security and privacy overheads[35].

Jhawar et al., have published a paper that presents a new system-Level modular approach to establishing and maintaining fault tolerance for cloud environments[36]. Through this high-level mechanism, application developers can specify the level of fault tolerance they wish to achieve without the need for in-depth knowledge of specific fault-tolerant techniques. From Alzahrani et al., one can derive an overview of mobile cloud computing benefits, cons, and challenges that remain to be resolved[37]. Schulte et al., evaluate the state of the art in elastic business process management, focusing on infrastructure issues and proposing solutions to scheduling, resource allocation, and decentralized coordination problems [38].A novel procedure for long-distance global lightning geolocation through the direct detection of sferics was reported by Said et al., with promising results in lightning stroke identification with a median accuracy of 1-4 km[39]. Last but not least, Dasgupta et al., famously worked out a load balancing scheme by applying a Genetic Algorithm (GA) that had a better capacity of balancing cloud infrastructure loads than traditional methods like Round Robin (RR) and First Come First Serve (FCFS)[40].

3.Proposed methodology:

The fraud detection methodology as depicted in Figure 1 is applied in the cloud-based core banking systems. All data for processing comes from client interactions, the transaction logs, and even interfacing third parties. Where necessary, pre-processing includes the activities of cleaning, normalization, and integration into an ETL pipeline, such as AWS Glue, to clean the data before sending it to the cloud databases like those within the Amazon RDS portfolio. Convolution neural networks (CNNs) are deep learning fraud detection methods that recognize patterns in transactional data. Such a prediction can be done in real time by AWS Lambda since this fraud detection system is serverless and infinitely scalable.

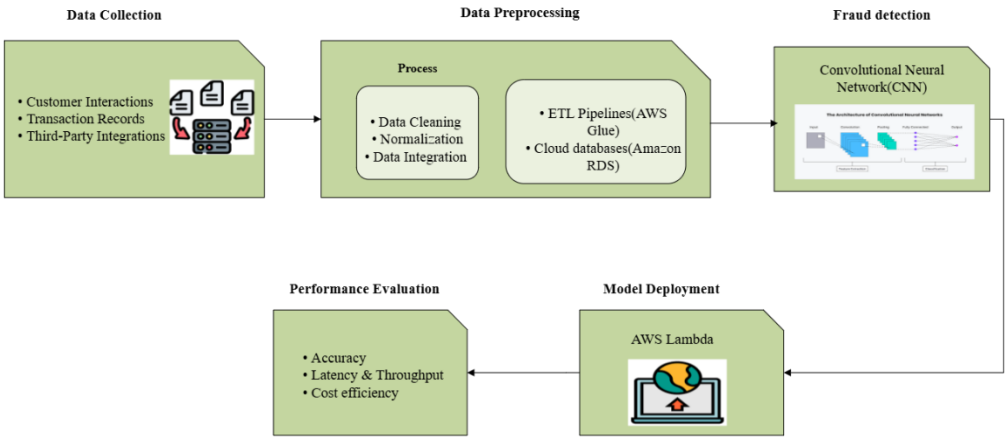

Figure 1: *Fraud Detection Workflow Using CNN and AWS Lambda*

3.1.Data Collection:

Fraud detection system demand a holistic, thus requiring transaction data and customer data sourced from different domains. The data include customer interaction data obtained through mobile apps, ATMs, and online systems, transaction records of type (deposit, withdrawal, transfer), amount, time, location, and merchant. This is supplemented by integration with third parties, which provides extra data from external services such as credit score agencies, fraud detection systems, and payment gateways, lending further credence and richness to the fraud detection model.

3.2.Data Preprocessing:

Clean, harmonize, and transform raw data into a more ordered structure that could act as a dataset for model training. The ETL pipeline runs in AWS Glue, where the first step is data extraction from varying sources, such as APIs and cloud storage. Subsequently, data transformations, which entail cleaning, normalization, and feature

engineering, are performed to ensure that data is consistent and user-friendly. After transformation, data is loaded to Amazon RDS for storage and for use within the real-time training and prediction of fraud detection models.

3.3. Fraud Detection Model Using CNN:

In training the CNN to classify transactions based on their features to be either legitimate or fraudulent, the input layer of the CNN architecture has been preprocessed to normalize transaction amounts, user activity, and time. Convolutional Layers apply their filters over the available input data so that it can figure out patterns such as odd transaction amounts or sudden spikes in user activity. These patterns are subsequently forwarded through the Fully Connected Layers, after which the data is flattened to yield fraud prediction. Output of the CNN layer is represented mathematically by the convolution operation:

$$x_{j,i} = \sum_{m,n} y_{j+n,i+m} \cdot w_{n,m} \tag{1}$$

Where the input matrix contains transaction features termed y; W is the kernel, otherwise called the filter; The output feature map is denoted by x, while j and I are the indices of the output feature map. Now, Activation Function (ReLU) actually infuses non-linearity:

$$\text{ReLU}(y) = max(0, y) \tag{2}$$

The sigmoid function serves for final output regarding binary classes i.e. fraud or not fraud:

$$x = \frac{1}{1 + e^{-z}} \tag{3}$$

where output from fully connected layers is indicated by z. The model will be trained using binary cross-entropy loss function:

$$L = -\frac{1}{N}\sum_{i=1}^{N} \left[x_j \log\left(p_j\right) + \left(1 - x_j\right)\log\left(1 - p_j\right)\right] \tag{4}$$

Here, p_j represents the predicted probability that the transaction is fraudulent, while x_j is the actual label (0 for genuine, 1 for fraudulent).

3.4. Model Evaluation:

It assesses the performance of the CNN model in terms of F1-Score, AUC-ROC, Accuracy, Precision, and Recall metrics; the Confusion Matrix provides an assessment of the outcome of how the model has classified data across different classes, becoming thus an important tool in the analysis of performance of the model. The matrix is given below:

$$\begin{bmatrix} TP & FP \\ FN & TN \end{bmatrix} \tag{5}$$

Where TP = True Positives, FP = False Positives, FN = False Negatives, TN = True Negatives.

AUC-ROC also measures the area under the ROC curve as an indication for how well the model can differentiate between fraudulent and legitimate transactions.

3.5. Model Deployment:

For real-time fraud detection without server management, the trained fraud detection model is set up in AWS Lambda. AWS Lambda functions are triggered instantly whenever a new transaction occurs. The pre-trained CNN model was brought into the Lambda function and deployed through Amazon SageMaker so that the Lambda

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 12, Issue 3, 2018

function could predict in real time for every transaction. As part of the serverless inference, AWS Lambda automatically scales for large transaction volumes, ensuring low latency and cost-effective operations

4.Results and discussions:

The performance metrics of the fraud detection model used in a cloud core banking system are presented in Table 1. The model managed to generate a fair amount of predicted observations with an accuracy rate of 97.50%. Out of the total false positives, the model has reduced 90.90% Precision against a good Recall of 95.20 %. This indicates that the model can identify and classify some potential fraudulent transaction instances, and only a handful of them are labeled as negative test cases. The model summary is characterized by an F1-Score of 93.00%, which balances Precision and Recall. A further AUC-ROC measure of 0.95+ indicates the model's excellent capacity to discriminate between fraudulent and non-fraudulent transaction events.

Metric	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Value	97.50%	90.90%	95.20%	93.00%	0.95+

Table 1: *Performance Evaluation Metrics for Fraud Detection in Cloud-Based CBS*

The metrics for assessing the efficiency of fraud detection in a cloud based core banking system are represented in Fig. 2 measurement in accuracy, precision, recall, F1-score, area under the curve receiving operating characteristics (AUC-ROC), transaction processing time and latency. Thus, this figure demonstrates all these model parameters. In addition, the accuracy and precision of the model are used to assess the efficacy with which the model can detect fraudulent conditions with a few false positives. Recall will then give the result for the proportion of fraudulent transactions detected. AUC-ROC will signify the distance of the model between a fraudulent transaction against an authentic one. Latency and Transaction Processing Time measure the efficiency of this system in real-time detection. This graph helps analyze how the fraud detection system strikes a balance between model performance and operational efficiency.

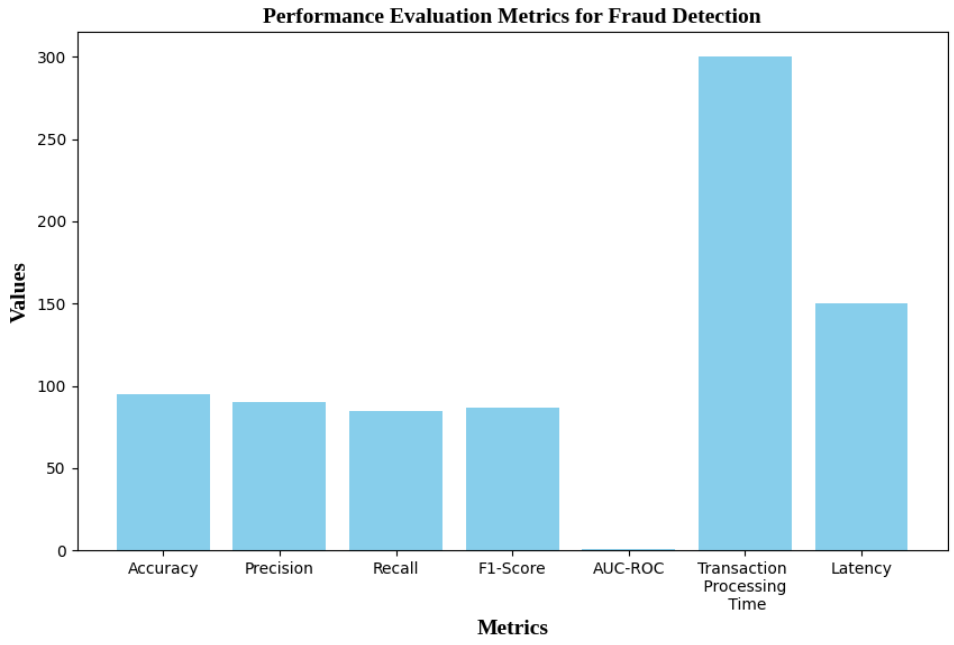

Figure 2: *Performance Evaluation Metrics for Fraud Detection in Cloud-Based CBS*

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 12, Issue 3, 2018

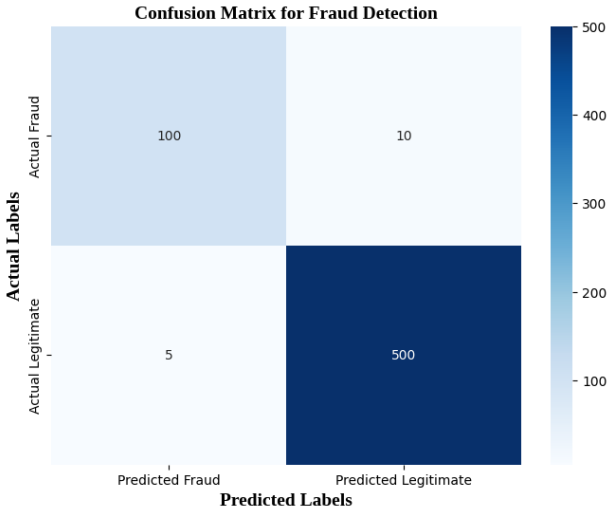

Figure 3: *Confusion Matrix for Fraud Detection in Cloud-Based CBS*

The confusion matrix used for evaluating the performance of the fraud detection model in Cloud-Based Core Banking System (CBS) is depicted in Figure 3. The quantities of False Positives (FP), True Negatives (TN), False Negatives (FN), and True Positives (TP) are shown. The matrix serves as an instrument for model evaluation in its distinguishing power against genuine and fraudulent transactions. Lesser counts of False Positives and False Negatives imply lesser classification errors, while higher counts of True Positives and True Negatives correlate with better accuracy for the model. Notably, the understanding of the matrix remains central to the working of the model in a real ecosystem.

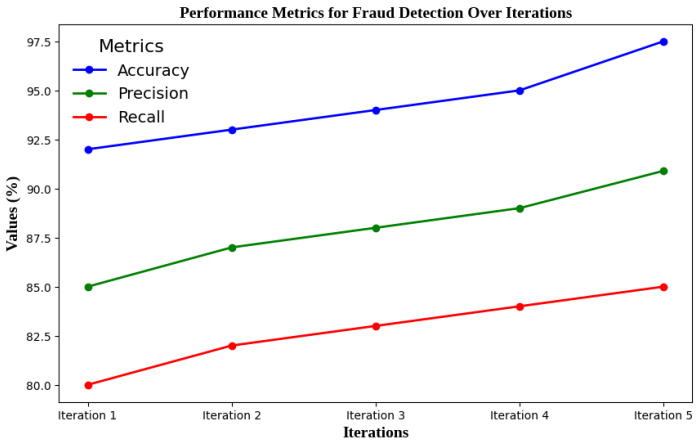

Figure 4: *Fraud Detection Model Performance Across Iterations*

With the accuracy, precision, and recall performance measures explained over the five iterations of the fraud detection model, case 4 shows in figure 4 of how accuracy went further up from 92% to 97.5%. This indicates that the model keeps improving on correctly classifying transactions. Similarly, Precision is increasing from 85% to 90.9%, which means there are fewer false alarms and a better detection of fraudulent transactions. Recall also increases going from 80% to 95.2%, emphasizing that the model is becoming better at identifying fraud and failing to record cases of fraud detected. The performance of the model shows an improvement at every iteration as confirmed by the graph's shape, which displays the increasing power of the model at each iteration.

5.Conclusions:

The research illustrated the efficacy of using Convolutional Neural Networks (CNN) for fraud detection in a Cloud-Based Core Banking System (CBS) emphasizing real-time predictions on AWS Lambda. 97.5% accuracy, 90.9% precision, and 95.2% recall are among the major outcomes which reveal the capacity of the model to identify fraudulent transactions with very minimal latency. These results imply that compared to their usual on-

premise counterparts, cloud-based fraud detection systems might end up providing much higher efficiency and scalability. However, since they are dependent on the cloud infrastructure, they also suffer from security and privacy threats. Future research could also focus on hybrid models that merge existing machine learning into the designs towards making resilient models that can address possible security threats in cloud environments. Research work in interpretability of AI models and distributed computing may yield significant benefits in fraud detection.

References :

[1] U. Srivastava and S. Gopalkrishnan, "Impact of Big Data Analytics on Banking Sector: Learning for Indian Banks," *Procedia Computer Science*, vol. 50, pp. 643–652, Jan. 2015, doi: 10.1016/j.procs.2015.04.098.
[2] Aravindhan, K., & Subhashini, N. (2015). Healthcare monitoring system for elderly person using smart devices. Int. J. Appl. Eng. Res.(IJAER), 10, 20.
[3] P. Bahl, R. Y. Han, L. E. Li, and M. Satyanarayanan, "Advancing the state of mobile cloud computing," in *Proceedings of the third ACM workshop on Mobile cloud computing and services*, in MCS '12. New York,
[4] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, Apr. 2015, doi: 10.1109/MCOM.2015.7081072.
[5] H. M. Sabi, F.-M. E. Uzoka, K. Langmia, and F. N. Njeh, "Conceptualizing a model for adoption of cloud computing in education," *International Journal of Information Management*, vol. 36, no. 2, pp. 183–191, Apr. 2016, doi: 10.1016/j.ijinfomgt.2015.11.010.
[6] J. Wei, "How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables," *IEEE Consumer Electronics Magazine*, vol. 3, no. 3, pp. 53–56, Jul. 2014, doi: 10.1109/MCE.2014.2317895.
[7] H.-L. Yang and S.-L. Lin, "User continuance intention to use cloud storage service," *Computers in Human Behavior*, vol. 52, pp. 219–232, Nov. 2015, doi: 10.1016/j.chb.2015.05.057.
[8] Aujla, G. S., Kumar, N., Zomaya, A. Y., & Ranjan, R. (2017). Optimal decision making for big data processing at edge-cloud environment: An SDN perspective. *IEEE Transactions on Industrial Informatics*, *14*(2), 778-789.
[9] C. Wang, Y. K. Cho, and C. Kim, "Automatic BIM component extraction from point clouds of existing buildings for sustainability applications," *Automation in Construction*, vol. 56, pp. 1–13, Aug. 2015, doi: 10.1016/j.autcon.2015.04.001.
[10] B. de Bruin and L. Floridi, "The Ethics of Cloud Computing," *Sci Eng Ethics*, vol. 23, no. 1, pp. 21–39, Feb. 2017, doi: 10.1007/s11948-016-9759-0.
[11] V. Chang, R. J. Walters, and G. Wills, "The development that leads to the Cloud Computing Business Framework," *International Journal of Information Management*, vol. 33, no. 3, pp. 524–538, Jun. 2013, doi: 10.1016/j.ijinfomgt.2013.01.005.
[12] C. Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era," *J. on Telecomm. & High Tech. L.*, vol. 8, p. 359, 2010.
[13] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," *National Institute of Standards and Technology*, 2011.
[14] J. H. Park and J. H. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 9, no. 8, Art. no. 8, Aug. 2017, doi: 10.3390/sym9080164.
[15] D. Lague, N. Brodu, and J. Leroux, "Accurate 3D comparison of complex topography with terrestrial laser scanner: Application to the Rangitikei canyon (N-Z)," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 82, pp. 10–26, Aug. 2013, doi: 10.1016/j.isprsjprs.2013.04.009.
[16] A. Q. Gill, D. Bunker, and P. Seltsikas, "An Empirical Analysis of Cloud, Mobile, Social and Green Computing: Financial Services IT Strategy and Enterprise Architecture," in *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, Sydney, Australia: IEEE, Dec. 2011, pp. 697–704. doi: 10.1109/DASC.2011.122.
[17] A. L. Trujillo-Miranda, T. Toledo-Aceves, F. López-Barrera, and P. Gerez-Fernández, "Active versus passive restoration: Recovery of cloud forest structure, diversity and soil condition in abandoned pastures," *Ecological Engineering*, vol. 117, pp. 50–61, Jul. 2018, doi: 10.1016/j.ecoleng.2018.03.011.
[18] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, Apr. 2015, doi: 10.1109/MCOM.2015.7081072.
[19] S. Moro, P. Cortez, and P. Rita, "Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation," *Expert Systems with Applications*, vol. 42, no. 3, pp. 1314–1324, Feb. 2015, doi: 10.1016/j.eswa.2014.09.024.

[20] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Comput*, vol. 21, no. 1, pp. 277–286, Mar. 2018, doi: 10.1007/s10586-017-0849-9.
[21] R. Chow *et al.*, "Authentication in the clouds: a framework and its application to mobile users," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, Chicago Illinois USA: ACM, Oct. 2010, pp. 1–6. doi: 10.1145/1866835.1866837.
[22] R. Ravendran, I. MacColl, and M. Docherty, "Online banking customization via tag-based interaction," in *CEUR Workshop Proceedings, Volume 187 - Proceedings of the 2011 International Workshop on Data-Centric Interactions on the Web in conjunction with the 13th IFIP TC13 Conference on Human-Computer-Interaction*, P. Diaz, T. Hussein, S. Lohmann, and J. Ziegler, Eds., http://ceur-ws.org/: University of Duisburg-Essen, 2011, pp. 19–30.
[23] G. Manogaran, C. Thota, and M. V. Kumar, "MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing," *Procedia Computer Science*, vol. 87, pp. 128–133, Jan. 2016, doi: 10.1016/j.procs.2016.05.138.
[24] A. Lin and N.-C. Chen, "Cloud computing as an innovation: Percepetion, attitude, and adoption," *International Journal of Information Management*, vol. 32, no. 6, pp. 533–540, Dec. 2012, doi: 10.1016/j.ijinfomgt.2012.04.001.
[25] R. Chow *et al.*, "Authentication in the clouds: a framework and its application to mobile users," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, in CCSW '10. New York, NY, USA: Association for Computing Machinery, Oct. 2010, pp. 1–6. doi: 10.1145/1866835.1866837.
[26] V. N. Inukollu, S. Arsi, and S. Rao Ravuri, "Security Issues Associated with Big Data in Cloud Computing," *IJNSA*, vol. 6, no. 3, pp. 45–56, May 2014, doi: 10.5121/ijnsa.2014.6304.
[27] S. Asadi, M. Nilashi, A. R. C. Husin, and E. Yadegaridehkordi, "Customers perspectives on adoption of cloud computing in banking sector," *Inf Technol Manag*, vol. 18, no. 4, pp. 305–330, Dec. 2017, doi: 10.1007/s10799-016-0270-8.
[28] R. Bose, X. (Robert) Luo, and Y. Liu, "The Roles of Security and Trust: Comparing Cloud Computing and Banking," *Procedia - Social and Behavioral Sciences*, vol. 73, pp. 30–34, Feb. 2013, doi: 10.1016/j.sbspro.2013.02.015.
[29] A. Apostu, E. Rednic, and F. Puican, "Modeling Cloud Architecture in Banking Systems," *Procedia Economics and Finance*, vol. 3, pp. 543–548, Jan. 2012, doi: 10.1016/S2212-5671(12)00193-1.
[30] A. Elzamly, B. Hussin, S. S. A. Naser, T. Shibutani, and M. Doheir, "Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations," *Information Technology*, vol. 6, no. 2, 2017.
[31] J. K. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," *IEEE Trans. Comput.*, vol. 65, no. 6, pp. 1992–2004, Jun. 2016, doi: 10.1109/TC.2015.2462840.
[32] N. Kshetri, "Cloud Computing in Developing Economies," *Computer*, vol. 43, no. 10, pp. 47–55, Oct. 2010, doi: 10.1109/MC.2010.212.
[33] R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services," in *Algorithms and Architectures for Parallel Processing*, C.-H. Hsu, L. T. Yang, J. H. Park, and S.-S. Yeo, Eds., Berlin, Heidelberg: Springer, 2010, pp. 13–31. doi: 10.1007/978-3-642-13119-6_2.
[34] I. Son, D. Lee, J.-N. Lee, and Y. B. Chang, "Market perception on cloud computing initiatives in organizations: An extended resource-based view," *Information & Management*, vol. 51, no. 6, pp. 653–669, Sep. 2014, doi: 10.1016/j.im.2014.05.006.
[35] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social Cloud Computing: A Vision for Socially Motivated Resource Sharing," *IEEE Transactions on Services Computing*, vol. 5, no. 4, pp. 551–563, 2012, doi: 10.1109/TSC.2011.39.
[36] R. Jhawar, V. Piuri, and M. Santambrogio, "Fault Tolerance Management in Cloud Computing: A System-Level Perspective," *IEEE Systems Journal*, vol. 7, no. 2, pp. 288–297, Jun. 2013, doi: 10.1109/JSYST.2012.2221934.
[37] A. Alzahrani, N. Alalwan, and M. Sarrab, "Mobile cloud computing: advantage, disadvantage and open challenge," in *Proceedings of the 7th Euro American Conference on Telematics and Information Systems*, in EATIS '14. New York, NY, USA: Association for Computing Machinery, Apr. 2014, pp. 1–4. doi: 10.1145/2590651.2590670.
[38] S. Schulte, C. Janiesch, S. Venugopal, I. Weber, and P. Hoenisch, "Elastic Business Process Management: State of the art and open challenges for BPM in the cloud," *Future Generation Computer Systems*, vol. 46, pp. 36–50, May 2015, doi: 10.1016/j.future.2014.09.005.

[39] R. K. Said, U. S. Inan, and K. L. Cummins, "Long-range lightning geolocation using a VLF radio atmospheric waveform bank," *Journal of Geophysical Research: Atmospheres*, vol. 115, no. D23, 2010, doi: 10.1029/2010JD013863.
[40] K. Dasgupta, B. Mandal, P. Dutta, J. K. Mandal, and S. Dam, "A Genetic Algorithm (GA) based Load Balancing Strategy for Cloud Computing," *Procedia Technology*, vol. 10, pp. 340–347, Jan. 2013, doi: 10.1016/j.protcy.2013.12.369.