Journal of Positive School Psychology http://journalppw.com
2022, Vol.6, No.4, 2340-2349

Prediction of fraud in electronic payment system through Machine Leaning model

Manoj kumar Shamrao Barbhai[1];Dr. Yogesh kumar sharma[2]; Dr. Shraddha Bhushan Sable[3]

[1]Research Scholar Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan
[2]Dean, School of Engineering & Technology
[3]Assistance Professor, Tilak Education Societ, S.K. college of Science and Commerce, Nerul, Navi Mumbai, Maharashtra

Abstract:

In this paper, we address unwavering quality issues in three-level frameworks with stateless application servers. For these frameworks, astructure called e-Transaction has been as of late proposed, which indicates a bunch of beneficial start to finish unwavering quality assurances. In thisarticle, we propose an inventive circulated convention giving e-Transaction ensures in the overall instance of different, independentback-end data sets (common of situations with different gatherings required inside an equivalent business process). Uniquely in contrast to existingproposition adapting to the e-Transaction structure, our convention depends on no suspicion on the precision of disappointment recognition.Consequently, it uncovers appropriate for a more extensive class of dispersed frameworks. To accomplish such an objective, our convention takes advantage of an imaginative planfor dispersed exchange the board (in view of impromptu boundary and simultaneousness control systems), which we present Machine learning model inthis paper. Past giving the confirmation of convention accuracy, we additionally examine hints on the convention coordination with ordinaryframeworks (e.g., data set frameworks) and show the negligible upward forced by the convention.

Keywords: Barriers, Electronic Transactions, Customers, Banks, Machine Learning

1. Introduction

The advancement of online business showed a more noteworthy requirement for installment framework to get clients' monetary information while sending it over the Internet. From that point forward, different installment frameworks have been created. However, with the progression in the internet and innovation, safeguarding clients' monetary information isn't the main issue. Monetary cheats detailed throughout the years because of programmers, spammers, extortion vendors and organize breaks have turned into a central issue. To resolve these issues, current web-based installment frameworks like Verified by Visa and SecureCode depend on state of the art advances for distinguishing counterfeit exchanges and misrepresentation shippers. In doing as such, they follow a methodology where clients' installment data is first shipped off traders and afterward the vendors divert it to installment doors. This methodology related to different advances functions admirably as traders and installment passages discuss straightforwardly with one another and know about clients, buys and installments. However, autonomously, this approach doesn't work with in safeguarding clients' monetary information from misrepresentation traders. Rather it makes the whole framework defenseless to encroachment/interruption.

At the point when clients send their installment data (hashed/scrambled) to traders, they don't know how that data goes over the Internet and is handled by a vendor. Shippers can save the encoded/hashed monetary data of clients and later unscramble it. It could likewise be conceivable that a vendor's server is being compromised and he is totally uninformed about it. Then again, most banks depend on secret key based admittance and encryption strategies to get clients' information. A bank, nonetheless, can't ensure that a client's monetary data has not been compromised assuming that data has gone

through a shipper's server prior to arriving at an installment passage/bank.

Thinking about these variables, we derive that sending clients' monetary data to installment passages by means of traders opens it to extra organizations vulnerable to data breaks and assaults. Subsequently, to stay away from this weakness, we foster an alternate methodology for installment frameworks in which clients straightforwardly send their installment data to installment passages. This way a dealer gets compensated for his sold things without getting a client's installment data, not even in encoded/hashed structure.

2. Inhibitors of E-Commerce and Lack of Legislation

A significant component which has harmed on the reception of online business in Saudi Arabia is the absence of regulation and the absence of a steady lawful climate. There are, nonetheless, other restraining factors that are additionally of most extreme significance to the fruitful development of online business which will likewise be illustrated. It is believed that the restricted cooperation of internet business can be because of inborn issues that face non-industrial nations. These issues incorporate training potential open doors, abundance, admittance to Internet frameworks and organizations. As referenced before, Saudi Arabia has put resources into its broadcast communications foundation to the point that it can uphold electronic trade, so here Saudi Arabia is advancing. A few other general obstructions to the advancement of online business notwithstanding, are specialized, hierarchical, financial, political, and social. Information on specific social subtleties are essential in grasping the convoluted course of taking on electronic trade. It is believed that as more countries understand the potential that electronic business has in helping global exchange, there ought to be a sluggish abatement in the previously mentioned obstructions.

Before examining the absence of certain and clear electronic trade regulation in Saudi Arabia, it is important to show that there are likewise numerous other hindering variables for the sluggish reception of electronic business which need referencing. Other than the previously mentioned absence of regulation, a few other widespread obstructions to the advancement of internet business are specialized, hierarchical, financial, political, and social. It is imagined that as more countries understand the potential that electronic business has in helping global exchange, there ought to be a sluggish lessening in the previously mentioned obstructions. It is critical to take note of that other less unmistakable issues to the reception of electronic trade exist, and information on specific social subtleties are fundamental in fathoming the convoluted course of embracing electronic business.

Another repressing boundary to the reception of online business incorporates a social inclination of directing business up close and personal. A further boundary is the pattern for Saudi's to utilize the Internet only for getting to information and not as a channel for shopping. Also, there are hindrances in the installment technique choices which are negligible as well as the predominance of English which actuates dread into the purchasers there. There is additionally a genuine hesitance to change shopping conduct, also the anxiety toward facing a challenge and shopping on the web. The nature of client care and after deal support, are likewise referenced as frail and contributing variables to the sluggish development of internet business.

3. Factors affecting the adoption of e-commerce

There have been examinations that have explored how SMEs view web based business, the possible advantages to be acquired from taking part in it, the apparent disincentives that hinder them from embracing it, the triggers that drove them into taking on, how they approached the course of reception, and what they accomplished from taking on. The many advantages apparent to get from taking part in online business are viewed as triggers or empowering influences to the reception of internet business. Seen benefits, nonetheless, are not by any means the only explanation organizations participate in internet based business. There are in many cases different triggers that push them.

Outside drives, for example, government expecting providers to bargain just electronically, can be huge triggers (Department of Industry and Technology 2001). As indicated

by Ah-Wong et al. (2001), the triggers or empowering influences or drivers of web based business are seen as the innovative, authoritative and legislative elements which urge internet business to blast.

Altogether, more prominent business development appeared to underlie SMEs' choices to fuse internet business into their business methods. As per the majority of the examinations done, SMEs, whether or not they have embraced online business, see an enormous scope of expected motivators to be acquired from taking on past those portrayed by Ah-Wong et al. These are talked about in the accompanying area.

Seen motivations for the reception of web based business

Huge organizations and government offices have promptly embraced internet business. While it is generally acknowledged that there are many benefits to be acquired from partaking in it, SMEs have been safe. There have been a lot of examinations that have explored the advantages organizations see they will accomplish from taking on web based business.

4. Related Work

To confirm the practicability of the current installment innovations, Lacmanovi et al. [4], in 2010, presented the benefits of some radio recurrence (RF)- based contactless installment strategies supporting Visa Contactless, MasterCard Pay Pass, and Express Pay. As well as exploring RF innovation, the creators examined a few contactless card issues like trader reception, the global image, and the promising strategy called close field correspondence (NFC). They likewise examined security concerns, including abuse of lost cards, extortion assurance, and the necessary power properties, i.e., shared validation, solid data security, a solid contactless gadget security, approved data access, insurance against exchange replay, support for biometric confirmation, and solid help for data protection. Afterward, Chen et al.

[8] proposed a versatile installment framework for conventional in-store conditions. They took on different procedures, for example, the Citizen Digital Certificate PKI and the NFC secure component inside a SIM card, to get the course of their proposed installment plot. In [10], Ail and Awal introduced a NFC-based convention installed with a validation plan to get the versatile installment process under GSM organizations. A Hash work strategy is taken advantage of to create codes and trustworthiness keys as the urgent part in the proposed framework. The idea of the security component, i.e., a Trusted Services Manager in the proposed plot, is likewise taken on to ensure secure portable correspondence.

In 2012, Mainetti et al. [5] fostered a NFC miniature installment framework in light of the shared NFC working mode for Android cell phones, called IDA-Pay. The proposed IDAPay framework ensures the security of versatile to-POS micropayment administrations. Rather than a security component, an encoded record, called a Credit Card File, is kept up with in the telephone memory for each web-based exchange, in which the RSA calculation with 2048 cycle keys is taken on to get the information. What's more, an IDAPay POS application is introduced for installment information trade, while an IDA-Pay door is answerable for sending the installment solicitation to the right Mastercard network endpoint. A testing situation is then utilized to exhibit the framework's adequacy.

The next year, Kazan and Damsgaard [7] proposed a system for connection examination and the fundamental parts of an effective computerized installment stage. They investigated three contactless installment frameworks utilized in the European market, i.e., Saving Bank's Girogo, Orange France, and Yapital, to analyze the approval of the proposed structure. Around the same time, Cha and Kim [6] planned a NFC-based miniature installment framework for secure exchanges. In their installment framework, a tokenization procedure is used to help client protection while a message digest-based confirmation conspire is proposed to further develop security and effectiveness.

Accordingly, Blass et al. [9] presented a RFID-based installment convention with client protection safeguarding. In the convention, the labels make legitimate coins at every exchange occurrence as opposed to putting away them ahead of time. The proposed framework utilizes precomputed challenge-reaction matches to finish the peruser validation. This makes it

inconceivable for foes to develop (or take coins) from authentic clients of the framework. Furthermore, the untraceability of a progression of resulting exchanges relating the client with a similar tag is ensured.

In 2014, To and Lai [15] researched the situation with portable banking and installment in China and set forward two contentions, i.e., 1) organizations should take advantage of a protected stage to improve purchasers'
readiness to utilize portable installment; and 2) responsibility and credit regulations should be acclimated to decrease gambles for shoppers and support the reception of versatile banking and installment in China. From that point onward, Magnier-Watanabe [12] explored the outcome of portable installment frameworks according to the viewpoint of regulative, standardizing, and mental institutional transporters. The instance of a portable installment framework utilized in Japan, Mobile Suica, is acquainted with show how a tight institutional fit can guarantee wide acknowledgment. Five partners are introduced, including handset makers, portable organization administrators, specialist co-ops, traders, and clients. This case exhibits that reception by end clients relies upon reception by the versatile installment's different partners recently referenced. In [13], to give security assurance and element confirmation, Abughazalah et al. introduced a portable installment conspire for NFC-empowered cell phones. Powerful plans, for example, once passwords and the Universal Integrated Circuit Card with a protected component giving
alter safe keys and solid cryptographic activity, are used as the center security parts. The creators then analyze the framework by means of the Casper FDR method and the determined
results exhibit its strength. As of late, Ojetund et al. [14] proposed a versatile impromptu organizations based portable installment framework which is infrastructureless and considers secure exchanges among clients in calamity regions. The proposed conspire uses an underwriting based instrument to ensure every exchange and simultaneously gives checking in light of area data. Exchange legitimacy and unwavering quality can consequently be accomplished. Afterward, to give secure web exchanges through cell phones, Sung et al. [11] presented the idea of the Transaction Certificate Mode (TCM), which is a product token supporting shared verification for versatile installments in circumstances of taken, acquired, and tainted cell phones. Then, at that point, a TCM-based shared verification convention is proposed to convey solid framework strength. In a word, the proposed TCM mode can be taken on to uphold an exceptionally solid and simpleto-use installment climate and at the same time further develop the calculation productivity.

In this review, we centeraround the plan and execution of certificateless computerized signature conspire for portable installments with wearable hardware. Here, we present the cutting edge of certificateless advanced signature. In 2014, the Gong and Li [27] introduced a CLS plot without utilizing bilinear pairings to seek after the heartiness and productivity during the framework tasks. The creators guarantee that their plan is secure against the super sort I and II enemies through a proof led by arbitrary prophet. Sadly, the proposition isn't hearty against super kind I foe [29]. Afterward, Tsai et al. [26] showed a better CLS conspire which depends on the plan proposed by He et al. [30]. The proposed technique not just gives preferred security over He et al's. CLS plot however conveys calculation effectiveness as just the activity of ECC-based point expansion is taken advantage of. Then, Wang et al. [28] presented a CLS conspire which is more productive than the plans introduced previously. The creators cut some calculation cost by means of a recently planned activity processes for signature age and check. All things considered, Wang et al's. CLS conspire is defenseless against a super sort I enemy [3]. That is, the protection from the mark phony assault isn't given. In [25], the creator proposed a certificateless short mark plan to fit for low band width correspondence climate. The proposed conspire is proficient and appropriate to gadgets with obliged capacity limit and gives vigorous protection from super kind I and II enemies also. It is by all accounts a promising up-and-comer procedure for protecting versatile installments with wearable gear. Nonetheless, because of the reception of bilinear matching crypto-activity, the calculation execution and the framework versatility is subsequently restricted.

5. Creating a Machine Learning Payment Fraud Model

Dataset Preparation

Before you can do anything more, you want to set up a dataset. By and large, the information focuses you use should be physically marked as either authentic or fake.

Your file of past installments, which has previously been marked by your security group, will make for an ideal dataset.

The greater (and better caliber) the pool of information you will prepare your brain network on, the more precise and proficient your framework will be.

Presentation of Features

Then, you should present highlights, which are information focuses depicting client conduct and giving you a reasonable sign that something is off-base with the exchange.

The most well-known highlights in installment handling are:

- Client personality
- Request data
- Installment strategy
- Area data

Having an enormous, pre-arranged corpus of deceitful installment elements will assist your framework distinguish false installments effortlessly from the very beginning.

Calculation Training

After highlights are presented, you really want to prepare the calculation on a preparation set of authentic information. When the preparation stage is finished, you will have a completed model that can begin recognizing fake installments.

The greater the preparation set, the better and more exact the framework will be.

Constant Improvement

During the primary phase of its activity, your security group should screen the framework and ensure that it is playing out the manner in which it ought to.

An extraordinary security group can likewise log the calculations' slip-ups as a whole and mistakes. These will be marked and added to the dataset that will be utilized to prepare another form of the model.

Because of these activities, the framework will turn out to be endlessly better over the long haul.

As may be obvious, preparing up a ML calculation is in no way, shape or form simple and can be over the top expensive with regards to both worker hours and assets. Fortunately, outsider arrangements like SDK. money's own personal Anomaly Detection and Fraud Prevention frameworks exist to assist organizations with exploiting the most recent improvements in AI advances at a negligible expense.

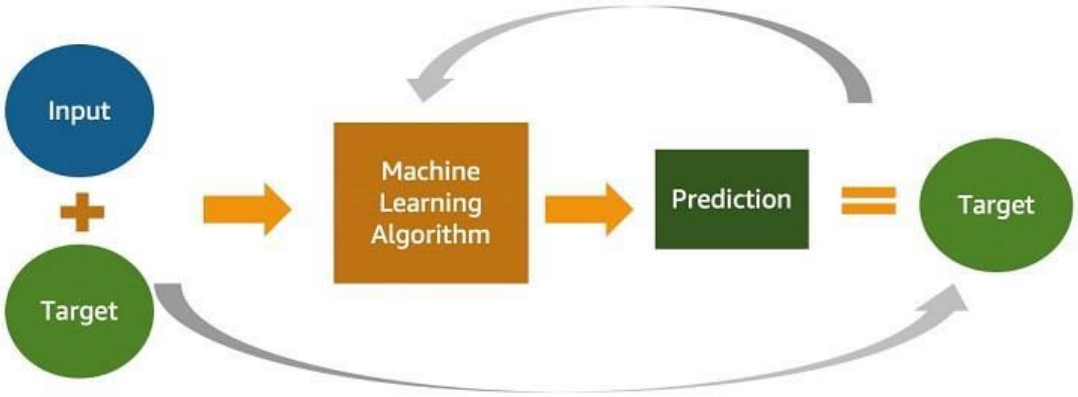

Figure 1 Machine leaning model

Machine Learning Models

The five most well-known ML models are arbitrary timberland, support vector machine, k-closest neighbors, brain organizations, and profound brain organizations. How about we take an elevated perspective at them all.

Irregular woodland

Perhaps the best illustration of instinctive naming in AI, an arbitrary backwoods is basically an assortment of isolated choice trees that are "developed" utilizing the preparation set. Whenever a piece of information should be grouped, every one of the choice trees will tell the timberland that it is so near its group. The timberland then picks the tree that gave the new piece of information the most votes.

With regards to installment misrepresentation, you can make a woods loaded up with different normal and not so normal sorts of exchanges. Whenever another exchange happens, the irregular timberland will quickly let your group know sort of exchange it.

Support vector machine

Another well known arrangement strategy is the help vector machine (SVM). In this technique, each element is introduced as a direction point. Every information thing is plotted as a point on a pivot of elements.

If we had any desire to make an order of all exchanges in view of two factors, for example, account age and installment total, we'd plot the two factors in a 2D space where each piece of information would have two directions.

Huge installments from another record would be named as high-risk. More modest installments from more seasoned records would be named as being more secure.

K-closest neighbors

Another basic, yet viable calculation is K-closest neighbors. It stores generally accessible cases and afterward arranges all new cases by means of a greater part vote from its K neighbors. The case relegated to another class will be the most well-known among its K closest neighbors as estimated by a distance work.

This framework is basically the same as the manner in which we instinctively group things as individuals. Suppose your bank gets another corporate client. This client is an individual from different industry associations, has accounts in a wide assortment of different banks, and routinely works with a significant number of your best clients. Similar people are attracted to one another. You and your security group instinctually realize that this client is authentic, in light of the fact that their "neighbors" are reliable.

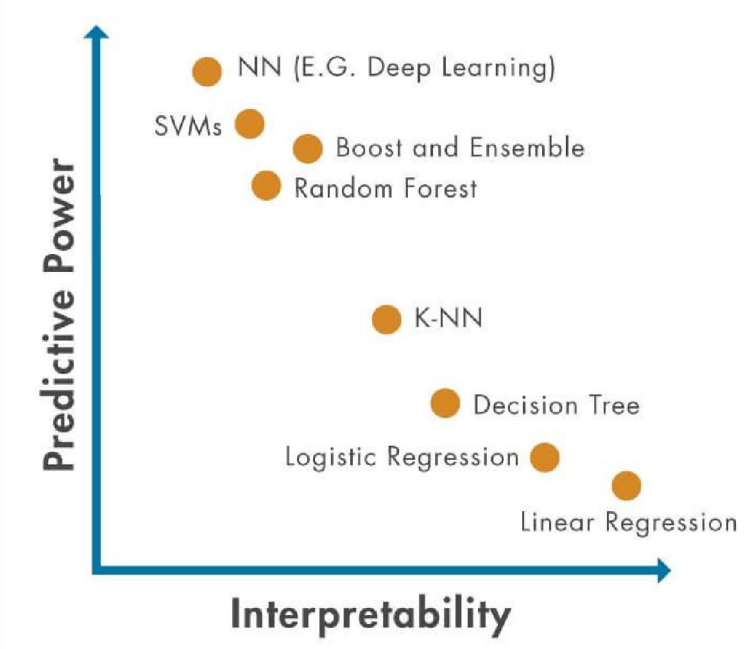

Figure 2 Machine leaning model performance comparsion

Brain organizations

Brain networks depend on a model of the human cerebrum. They are intended to perceive designs in crude information. Because of this, they can help organizations characterize and bunch immense measures of data rapidly and effectively.

Just stockpile a marked informational index to a brain organization and it will actually want to bunch future information as per likenesses without the requirement for you to add any extra elements (despite the fact that highlights can in any case be utilized to support the model).

Profound brain organizations

White ordinary brain networks are incredible for a great deal of arranging work, they can never be imaginative. That is the place where profound brain networks come in.

Being a considerably more convoluted and many-layered framework than normal brain organizations, profound brain organizations can likewise do much more. Organizations use them for such things as examination, anticipating future results, tackling inventive reasoning undertakings, and in any event, making workmanship.

Likewise, profound brain networks don't require however much direction that their customary brain organizations and might work with totally unlabeled informational indexes. And that implies that you can utilize profound nonpartisan organizations to take care of issues you, at the end of the day, don't have the foggiest idea how to settle.

Instances of profound brain networks incorporate the Deep Dream Generator, YouTube and Tic-Tac, as well as Sony CSL's music-creation calculation.

Daddy's Car, a Beatles-style tune produced by the Sony CSL AI

Profound learning extortion counteraction frameworks are still to some degree uncommon, yet the innovation has a ton of potential to change the manner in which monetary frameworks work and establish a lot more secure working climate for monetary organizations and their clients.

AI based extortion counteraction is an astonishing new advancement in the avoidance of illegal installments.

By supplanting obsolete rule-based frameworks with present day AI arrangements, banks and installment processors can lessen the misfortunes they bring about because of misrepresentation, bring down their security framework related expenses, and decrease installment contact for their clients.

Concerning the organizations that are reluctant to switch, the expenses related with keeping up with their heritage installment extortion frameworks will ultimately offset the venture important to present the more current framework. It is anticipated that all major monetary industry players will ultimately change to AI based installment misrepresentation avoidance frameworks.

6. Fraud detection using machine learning: Use cases

As of now, organizations work on extortion identification frameworks that consolidate AI and man-made reasoning. Utilizing current extortion insurance frameworks fueled by ML, numerous enterprises can guard their funds. There are now some misrepresentation recognition answers for FinTech, internet business, banking, medical care, web based gaming, and different ventures. Regardless of your industry, there's generally a method for profiting from AI and ML. AI calculations can handle immense measures of information and draw designs for each business to shield it from extortion. For example, AI assists internet gaming organizations with recognizing account takeovers and different tricks by following examples in a player's in-game way of behaving.

Capgemini claims their ML misrepresentation discovery framework can diminish extortion examination time by 70% while expanding precision by 90%. Another ML extortion counteraction arrangement supplier, Feedzai, claims that a thoroughly prepared AI arrangement can distinguish and forestall 95% of all misrepresentation while limiting how much human work expected during the examination stage.

Huge organizations like Airbnb, Yelp, and Jet.com are as of now utilizing AI answers for get bits of knowledge from large information and forestall issues like phony records, account takeover, installment misrepresentation, and advancement misuse. AI deals with all the

messy work of information examination and prescient investigation and permits organizations to develop and foster protected from extortion.

7. Conclusion

Organizations all around the world have proactively begun utilizing information science to forestall monetary misrepresentation. AI is as of now the most encouraging inventive apparatus that can assist organizations with forestalling deceitful tasks that lead to more noteworthy misfortunes every year. However aside from executing present day extortion discovery arrangements, organizations likewise need current and secure FinTech administrations and custom programming advancement benefits that are more enthusiastically for fraudsters to control. An obsolete monetary framework is generally loaded with provisos pranksters can utilize. Fortunately, AI can possibly further develop bank misrepresentation location with information investigation and help essentially every industry.

References

[1]. Jiangtao Li and Ninghui Li. OACerts : Oblivious Attribute Certificates, CERIAS and Department of Computer Science, Purdue University

[2]. Mohamed Nabeel, Elisa Bertino. CloudMask : Private Access Control in the Cloud, Purdue University, West Lafayette, Indiana, USA

[3]. Ning Shang, Mohamed Nabeel, Federica Paci, Elisa Bertino. A Privacy-Preserving Approach to Policy-Based Content Dissemination, Purdue University, West Lafayette, Indiana, USA

[4]. TorbenPryds Pedersen. Non-interactive and information theoretic secure verifiable secret sharing in CRYPTO'91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, London, UK: Springer-Verlag, 1992, pp 129-140

[5]. Dalal, S. &Athavale, V. (2012). Analysing Supply Chain Strategy Using Case-Based Reasoning. Journal of Supply Chain Management Systems, 1(3), 40-48.

[6]. Dalal S., Agrawal A., Dahiya N., Verma J. (2020) Software Process Improvement Assessment for Cloud Application Based on Fuzzy Analytical Hierarchy Process Method. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol. 12252. Springer, Cham. https://doi.org/10.1007/978-3-030-58811-3_70

[7]. Seth B., Dalal S., Kumar R. (2019) Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage. In: Kumar R., Wiil U. (eds) Recent Advances in Computational Intelligence. Studies in Computational Intelligence, vol 823. Springer, Cham.

[8]. S. Pradeep and Y. K. Sharma, "A Pragmatic Evaluation of Stress and Performance Testing Technologies for Web Based Applications," in 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 399–403.

[9]. Panthee, M., & Sharma, Y. K. (2019). Review of e-government implementation. International Journal of Recent Research Aspects, ISSN: 2349-7688, 6(1), 26–30.

[10]. Y. K. Sharma and M. D. Rokade, "Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic.," IOSR Journal of Engineering, pp. 63-67, 2019.

[11]. Bijeta Seth, Surjeet Dalal, Dac-Nhuong Le, VivekJaglan, NeerajDahiya, Akshat Agrawal, Mayank Mohan Sharma, Deo Prakash, K. D. Verma, Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm, Computers, Materials & Continua, Vol.67, No.1, 2021, pp.779-798, doi:10.32604/cmc.2021.014466

[12]. Sunita Saini, Dr. Yogesh Kumar Sharma, "LI-Fi the Most Recent Innovation in Wireless Communication", International Journal of Advanced research in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016.

[13]. Shuchen Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, Dept of ECE, Worchester Polytechnic Institute, Dept of ECE, Illinois Institute of Technology

[14]. Mohamed Nabeel, Ning Shang, John Zage, Elisa Bertino. Mask: A System for Privacy-Preserving Policy-Based Access to Published Content, Purdue University, West Lafayette, Indiana, USA

[15]. Gelman, A., & Hill, J. (2016). Data analysis using regression and multilevel/hierarchical models. Cambridge University Press.

[16]. Geurts, P., Ernst, D., &Wehenkel, L. (2016). Extremely randomized trees. Springer Science + Business Media, Inc..

[17]. Goodman, B., & Flaxman, S. (2016). European union regulations on algorithmic decision- making and a right to explanation. In ICML Workshop on Human Interpretability in Machine Learning.

[18]. Malik Meenakshi, NandalRainu, Dalal Surjeet, JalglanVivek and Le Dac-Nhuong 2021 Driving Pattern Profiling and Classification Using Deep Learning Intelligent Automation & Soft Computing 28 887-906.

[19]. Hastie, T., Tibshirani, R., & Friedman, J. (2002). The elements of statistical learning: Data mining, inference, and prediction. Biometrics.

[20]. Meenakshi Malik, RainuNandal, Surjeet Dalal, VivekJaglan and Dac-Nhuong Le, Deriving Driver Behavioral Pattern Analysis and Performance Using Neural Network Approaches, Intelligent Automation & Soft Computing, vol.32, no.1, 87-99, 2022, DOI:10.32604/iasc.2022.020249

[21]. Hidasi, B., Quadrana, M., Karatzoglou, A., &Tikk, D. (2016). Parallel recurrent neural network architectures for feature-rich session-based recommendations. In Proceedings of the 10th ACM Conference on Recommender Systems, 241–248.

[22]. Hochreiter, S., &Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8).

[23]. Hofmann, M. (2006). Support vector machines-kernels and the kernel trick. An elaboration for the hauptseminar reading club:support vector machines, 1 –16.

[24]. Hop, W. (2013). Web-shop order prediction using machine learning. Erasmus University Rotterdam.

[25]. Hsu, C.-W., Chang, C.-C., & Lin, C.-J. (2003). A practical guide to support vector classification (Tech. Rep.). Taipei 106, Taiwan: Department of Computer Science National Taiwan University.

[26]. Dalal, S., Seth, B., Jaglan, V. et al. An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. Soft Comput (2022). https://doi.org/10.1007/s00500-022-07099-4

[27]. Yogesh Kumar Sharma et al. "Designing enhanced Security Architecture for 5G Networks", International Journal of Management, IT & Engineering, ISSN: 2249-0558, Vol. 8, Issue 8(1), Pp. 73-83, Aug. 2018.

[28]. Yogesh Kumar Sharma et al. "Framework for Privacy Preserving Classification in Data Mining", Journal of Emerging Technologies and Innovative Research, ISSN: 2349-5162, Volume No. 5, Issue No. 9, pp. 178-183, Sept. 2018.

[29]. Yogesh Kumar Sharma et al. "Critical Study of Software Models Used Cloud Application Development", International Journal of Engineering & Technology, E-ISSN: 2227-524X, Volume No. 7, Issue No. 3.29, pp. 514-518, 2018.

[30]. Yogesh Kumar Sharma et al. "Project Virtualization Task Scheduler: A New Contribution to Green Cloud Computing", International Journal of Engineering Inventions (IJEI), ISSN (e):

2278-7461, ISSN (p): 2319-6491, Vol. 07, Issue 09, Pp. 43-46, Sept. 2018.

[31]. Yogesh Kumar Sharma et al. "Latest Review of Literature for Understanding Traditional Project Management Challenges and Need of Enterprise Cloud Project Management Practices", International Organization of Scientific Research Journal of Engineering (IOSRJEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719, Vol. 08, Issue 10, Pp. 1-5, Oct. 2018.

[32]. Yogesh Kumar Sharma et al. "Enhanced Technique for LSB Based Security in Digital Color Images Using Visual Cryptography", Journal of Computational Information Systems, ISSN: 1553-9105, Vol. 14, Issue 6, Pp. 81-88, Nov. 2018. 39. Paper published in International Journal of Management, Technology and Engineering, "Mobile Banking - How secure it is", ISSN: 2249-7455, Vol. 8, Issue XI, Pp. 24-28, November 2018.

[33]. Kukreja, S., Dalal, S. (2018). Performance Analysis of Cloud Resource Provisioning Algorithms. In: Saeed, K., Chaki, N., Pati, B., Bakshi, S., Mohapatra, D. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 563. Springer, Singapore. https://doi.org/10.1007/978-981-10-6872-0_57

[34]. Yogesh Kumar Sharma et al. "security-in-digital-images-using-visual-cryptography-scheme", Journal of Computational Information Systems, ISSN: 1553-9105, Volume No. 14, Issue No. 6, pp. 49-57, Nov. 2018.

[35]. S. Dalal and U. Jindal, "Performance of integrated signature verification approach: Review," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 3369-3373.

[36]. Yogesh Kumar Sharma et al. "Web Page Classification on News Feeds Using Hybrid Technique for Extraction", "Information& Communication Technology for intelligent system", Series Print ISSN 2190-3018, Series Online ISSN 2190-3026, Print ISBN 978-981-13-1746-0, Online ISBN 978-981-13-1747-7, Vol.-107, Issue-6, Pp.-399-405, DOI: https://doi.org/10.1007/978-981-13-1747-7_38, Dec. 2018.