Detecting Telecommunication Fraud with Visual Analytics: A Review

M Mohamed Amin¹, A Zainal², N F Mohd. Azmi³ and N A Ali⁴
¹,²,⁴School of Computing, Faculty of Engineering, UTM, Johor, MALAYSIA.
²Cyber Threat Intelligence Lab, Information Assurance & Security Research Group, UTM, Johor, MALAYSIA.
³Razak Faculty of Technology and Informatics, UTM, Kuala Lumpur, MALAYSIA.
E-mail: muhalim@utm.my

Abstract. The detection of anomalous events in large multivariate data is sought in many domains. Analysis of data is an important fraud detection procedure in detecting suspicious events and prevent attempts to defraud. While now the data is becoming more complicated and difficult as data scales and complexities increase than ever before, the rich insights within the data may be difficult to identify by traditional means and often remain hidden. People require powerful tools to extract valid conclusions from the data while maintaining trustworthy and interpretable results. Hence, various fraud detection approaches have started to exploit Visual Analytics (VA) techniques to reveal the hidden knowledge in such fraudulent activities. Interactive data visualization tools have substantial potential for making the detection of fraudulent transactions more efficient and effective by allowing the investigator to change the representation of data from text and numeric into graphics and filter out subsets of transactions for further fraud investigation. However, little research to date has directly examined the efficacy of data visualization techniques for fraud detection especially telecommunication fraud. In this paper, we present an overview of several fraud detection solutions that use data visualization techniques to detect fraudulent transactions in the telecommunication domain. The paper concludes by discussing how academic research might proceed in investigating the efficacy of interactive data visualization tools for fraud detection.

Keywords: Telecommunication fraud detection, visual analytics, multivariate, time-oriented

1. Introduction
Various types of fraud exist based on the nature of the fraud committed, and the methods vary based on their nature or their type of exploitation [1, 2]. There is a several number of fraud detection problems growing continuously or unstoppable [2] that concern for organisations of all sizes, across all regions and in virtually many sectors [3] including insurance, credit card, money laundering, computer intrusion, and telecommunications [4, 5, 6, 7, 8]. Fraud has become a worldwide phenomenon and prime issue of concern in the society that affects private enterprises as well as public entities [9, 10, 11]. Fraud may be defined as a dishonest or illegal use of services, to avoid service charges [12], or it can simply mean any activity that results in a gain in monetary benefit or unlawful advantage [13]. Telecommunication fraud has been a major challenge to the growth of the industry [14, 15] that suffers major losses due to fraud [4] all over the world. Since the beginning of
commercial telecommunications, the fraudsters have been causing huge loss of revenue to both the companies who offered these services and their customers [13, 5, 16, 17, 18] and it can affect the credibility and performance of telecommunication companies [9]. Usually, the fraud events are difficult to identify due to their sophisticated approach used by the fraudsters [19].

Analyzing and identifying such types of anomalous events normally focusses on the outlier of the patterns and samples that do not conform to expected behavior either anomalies or outliers [20] that classified as fraud. Not every fraudulent event can be classified as an outlier because sometimes attacks are hidden in known patterns to avoid detection by simple rule-based approaches [21]. Traditional audit methods involving the use of statistical sampling are often ineffective for discovering fraud [22]. Hence, the data mining procedure is performed to detect fraudulent transactions [23, 24] and needs to be examined more closely using some tools that may require considerable skill, as anomalies in data may not be readily apparent, except to the expert investigator. Visual analysis may facilitate identifying suspicious patterns of transactions in data. Interactive data visualization programs allow the investigator to more easily change the variables being graphed or focus on a subset of the data, or its format has now become readily available such as Tableau software [22].

Fraud investigators have recently recognized the importance of data visualization for fraud detection, and are starting to implement this technique in practice [25, 26]. Data visualization is especially important in the early stages of fraud investigation to perform efficient and effective data analysis and desires to better understand the relationships that may be present in a complex multivariate aspects of datasets, and become a subject of interest to the Visual Analytics (VA) community [21]. This is a proactive detection approach to search for data patterns that suggest fraudulent activity in [24]. Besides, [27] describe fraud detection as an open VA problem that requires visual exploration, discovery, and analysis. However, many of the current solutions involve mainly data mining techniques. VA approaches have the potential to improve these solutions by integrating human analysis into the process utilizing visual representations and interaction techniques [28]. Despite that, VA approaches are barely explored in the field of fraud detection [21].

The remainder of this article starts with a brief description of some related works on detecting fraud with VA approaches in general. It followed by a description of the visualization methods and interaction techniques, in general, to give a better understanding of the VA to gain insights about fraudulent events. Then, a review of existing works that use visualization techniques as part of their solution for fraud detection in telecommunication application domains. This article then elaborates on the benefits and shortcomings of VA approaches, and identify open challenges before concludes with future research directions might be proceeded in investigating the efficacy of interactive data visualization tools for fraud detection.

2. Related Works
Detecting for known fraudulent schemes as the suspicious events are insufficient due to the fraud techniques constantly changing to produce new patterns, and difficult to detect [29]. To this end, VA approaches can be applied to increase the outcome of new pattern discovery. Examples of review provided by [17, 30] that present the event detection using available tools for statistical fraud detection and identified the most used technologies in credit card fraud, money laundering fraud, telecommunication fraud, and computer intrusion. They classified the different fraud detection types based on the techniques of outlier detection; such as neural networks, expert systems, model-based reasoning, data mining, state transition analysis, and information visualization. In [31] presents techniques for event detection from Twitter streams using text stream visualizations by comparing the data type, text representation, and temporal drawing approach. However, they focus on different data types, namely text. Some reviews that focus specifically on data mining techniques for fraud detection research were also conducted by [32, 33, 34, 35].
In another perspective focusing on surveys of visual approaches for fraud detection, [36] surveyed that more than 50 papers present visualizations of financial data. They classified the visualizations, and outline ways to generate ideas for designing visualizations of financial data. A study in [22] presents a theoretical framework to predict fraud detection by applying VA techniques. They evaluated various visualization techniques and stated that different analysis process uses different visualization respectively. Another survey of visualizations and VA approaches also presented in [37] for exploring financial data in general.

Most of the existing surveys are mainly data mining-oriented and utilized visualization only as a visual aid for input and output data, and very general from the application point of view. In contrast, [21] conducted a survey that oriented towards the particular nature and characteristics of an application domain specifically for financial fraud event detection in multivariate time-oriented data. They outlined general similarities and differences in fraud detection tasks and approaches in financial domains. However, it can be adapted to tackle similar problems in other application domains. Based on works of literature, this present study will provide a review of some benefits and shortcomings of VA approaches in the telecommunication domain. Open challenges will be identified and concludes with possible opportunities for future research directions using potential interactive VA approaches tools for fraud detection.

3. Visual Analytics (VA)
VA that builds on human’s natural ability is remarkable to absorb a greater volume of information in visual than in numeric form and to discover certain interesting patterns and relevant outliers in multidimensional datasets that more easily derive insights about data [21, 38]. The main application domains normally characterized by their specific tasks in the fraud detection area such as in telecommunication, stock market, insurance, bank, and internal fraud detection. The internal fraud detection is also known as occupational fraud that involves internal employees commit internal access violations. Methods that represent data visually for application domains are the core aspect of the VA area, whereby the visualization is combined with human factors to explore the data interactively to gain insights about fraudulent events by using interaction techniques [39].

3.1. Visualization Methods
Visualization techniques enable a fraud investigator to see, explore, and understand a large amount of information. However, the efficiency of VA techniques varies concerning different tasks to identify fraudulent events within large multivariate datasets. The visualization methods that are used in the identified fraud detection approaches are line plots, node-link diagrams, bar charts, scatter plots, pixel-oriented diagrams, treemaps, heat maps, radar charts, parallel coordinates, box plots, polygons, and 3D visualization [21].

3.2. Interaction Techniques
When it comes to VA, the interaction technique employed by a solution is a determinant factor. [22] uses the term interactive data visualization techniques to contrast with static data visualization, which enables analysts to specify the format used to display information, select the information, or both. It has a strong influence on how analysts will explore the proposed technique as well as on the usability of the approach. Two groups of interaction techniques are representation tools and data selection tools. The first group consists of encode, reconfigure and connect, and while the latter group consists of select, abstract/elaborate, filter and explore. Another interaction techniques being used in the identified fraud detection approaches are undo/redo, change configuration, and no integration [21]. When developing a VA solution, the interaction techniques should be chosen by the visualization
techniques and tasks [40]. Determining this set of techniques is a critical task during visualization design. It impacts the quality of the analysts’ insights and the efficiency of the solution.

4. **Telecommunication Fraud Detection with VA**

   The work of [41] is the pioneer researchers who started a study in fraud detection from 1997. They introduced a hybrid adaptive fraud detection that tailored to bank fraud and telecommunication fraud detection. Moreover, it is a data mining-oriented and uses line plots during the analysis process. A set of monitors is generated to profile legitimate customer behavior using a rule-learning algorithm. One of the first studies which use VA techniques in the context of telecommunication fraud detection with the integration of visual and automated analysis is proposed by [38] by building visual interfaces to explore the data. They utilized a node-link diagrams, bar charts, and line charts in their work. To improve the node-link visualizations during interaction, they used clustering techniques.

   [42] presents an online fraud detection system based on a hierarchical regime-switching generative model using real mobile communication network data. They determine the probability of detection and false alarms using line plots. Therefore, they can be classified which alarm needs to be either kept or discarded.

   A work presents an approach to fraud detection in telecommunication based by combining a machine learning method with a basic VA approach to generates user profiling in [43]. Line plots are used in further analysis to compare different user’s profiles and, thus, detecting suspicious behaviors. Another review on the history of fraud detection from a big company presented by [44]. They also describe classes of fraud in the domain and propose VA models that support fraud detection in each of the different classes.

   [45] presented the design and implementation of Kerberos for a system to detect fraud over Voice over IP (VoIP) networks. This work is a rather analytical approach that aims for real-time detection of frauds. Kerberos allows the construction of pre-defined detection rules and the configuration of alarms. This work was experimentally evaluated using real-world data and presents good performance with different configurations.

   The most recent work found in this domain was [46]. The authors conducted a study to prove that VA approaches are beneficial to identify new, unexpected patterns using an open-source network analysis tool, Gephi [47]. Gephi allows exploratory analysis by creating interactive visualizations in terms of dynamic and hierarchical graphs. The VA approach by using a node-link visualization diagram tool can provide new insights into attacker behavior. This approach is based on statistical analysis or rule-based clustering and was experimentally evaluated using real Session Initiation Protocol (SIP) attack data collected over several years.

   Besides [46], we could not find many recent papers dealing with fraud detection in the telecommunication domain. Although the major part of the selected papers from the telecommunication domain being not recent, we still consider the VA approaches to be relevant in fraud detection context. Figure 1 summarized the most VA methods used in the study of telecommunication fraud detection within the years 1997 to 2018 by the number of studies in each particular year, respectively.
It clearly shows that line-plots is preferred VA methods compared to others. Perhaps, it simple and easy to display information as a series of data points that would help in identifying the behavior pattern in fraud detection.

5. Challenges and Opportunities in Telecommunication Fraud and VA

In this section, we present telecommunication fraud detection challenges and VA opportunities to address the challenges. Figure 2 illustrates the challenges that intertwined the complexity of data and tasks to identify fraudulent events within multivariate time-oriented data.

5.1 Hidden Features

In telecommunication fraud detection, the data is always multivariate, temporal, and comprises huge amounts of data consists of daily call transactions of customers, which are extremely very difficult and complicated to be visualized [29, 48]. This is partly since the data is not only multivariate but usually also always time-oriented that covers long periods. Moreover, in reality, it is hard to obtain real telecommunication transaction data or user’s call information due to privacy and security reasons. Therefore, the datasets often have some features hidden or changed to preserve customers’ privacy [29] even the private data would add to the accuracy of fraud detection [49]. Consequently, fraud detection is not a well-explored area in scientific research. To this end, visual aggregation techniques are often needed to display such rich datasets [21]. However, during analysis, the exploration of individual cases or short period analysis might still be interesting tasks. Thus, interaction techniques such as elaboration, exploration, and/or filtering are usually applied to utilize these visual scalability.
5.2 Hidden Patterns
All cases of telecommunication fraud can be viewed as fraud scenarios that are related to the way access to the network was acquired. However, given the most of telecommunication services and the cleverness of the fraudsters’ one may be confronted with diverse fraud techniques [49]. New fraud techniques are always being re-adapted so that the attempt is hidden as non-suspicious patterns of events [21]. So, detection techniques designed to detect one suspicious case within large of time-oriented and multivariate datasets may fail to detect other types of fraud [22]. It’s a challenging task that requires the visual and automatic approaches in an interactive multiple-coordinated exploration environment such as using 3D approaches. According to the summary as shown in Figure 3 by [21] exposed that no work in telecommunication uses the 3D approaches compared to other domains. Furthermore, 3D approaches are getting less popular recently that could be due to the difficulties to represent and interact with multivariate temporal data, and the perception of the 3D views may cause misleading impressions that can lead the analysts to wrong data interpretations. However, a systematic investigation of various interaction and visualization techniques according to particular tasks would open new possibilities to explore and analyze fraudulent behavior.

5.3 Monitoring Solutions
Besides, another challenge in the fraud detection within large of time-oriented and multivariate datasets is to find a monitoring solution to predict any possible future fraud with similar already detected fraud happened [50]. The suited solutions need to avoid false-positive and false-negative identification, which would waste the time of analysis, and which miss actual recurrent frauds, respectively [51]. Automated methods often fail to detect fraudulent behavior [21], because fraudsters are constantly changing their behavior to deceive monitoring and detecting systems. The fraud investigator could solve this using the VA approach by actively playing an active role with various steps in the knowledge generation process such as select automatic or analytical approaches, fine-tuning the parameter settings, and interactive exploration of the typically huge volumes datasets [21, 28, 52].

![Figure 3. Visualization methods used in fraud detection in 40 articles from 1997 to 2018 [21].](image)
5.4 Computation Capabilities

Providing visual support to interpret and understand the data, including predictive probabilities associated with them, become important as many existing applications need to solve predictive problems [54] such as to predict customer behavior in telecommunication. A large and complex data through a combination of Machine Learning (ML) and VA with interactive data visualization allow detecting suspicious behavior [29]. While current research has focused mainly on the efficiency of the visualization techniques to enable interactive exploration, this merging approach still under-explored [53], which promises a good synergy for motivating future research direction. ML algorithms enable us to tackle the dimension reduction, clustering, classification, and regression or correlation analysis tasks that frequently adopted in VA applications, and require the capabilities of computation and user expert. A general model and framework can be constructed to blend these two domains to develop a more powerful VA system with integrated ML.

6. Conclusion

Investigation of fraud is often required more details. The abilities of humans and the computer to identify patterns can be leveraged, whereby the human detect patterns interactively and the computer search for like instances across massive datasets tirelessly. In particular, by exploiting people’s abilities to deal with visual presentations, it may revolutionize the way of understanding large amounts of data by only looking for any unusual patterns that make an effective strategy for identifying new class of fraud attempted by the fraudsters. Effectiveness of fraud detection depends on the investigator’s ability to detect patterns in data that are suggestive of fraudulent transactions. Interactive data visualization tools have substantial potential for making the fraudulent transaction detection process at various stages become more efficient and effective, as they allow the investigator to navigate large datasets, change the representation of data, and filter subsets of data for further examination. VA literally maps the connection between different alternative solutions, leaving the opportunity to view these options in the context of the complete knowledge discovery process in fraud detection while maintaining the efficiency and accuracy in the context of detecting fraudulent transactions with interactive data visualization tools, and integration with ML to create more impactful systems to gain insight into data analysis.

Acknowledgment

The authors would like to express their appreciation for the support of the sponsors with Project No PY/2016/07336 (Q.J130000.2628.12J03).
References

[1] AlBougha M R. Comparing Data Mining Classification Algorithms in Detection of Simbox Fraud. M.sc. thesis, Department of Information Systems, St. Cloud State University, 2016. Culminating Projects in Information Assurance.

[2] Kinlan P. An Investigation into Real-time Fraud Detection in the Telecommunications Industry (2003-ish), January 2018.

[3] Misarwala F, Mukadam K, and Bhowmick K. Applications of Data Mining in Fraud Detection. *Int. Journal of Computer Sciences and Engineering*, 3(11):35–45, 2015.

[4] Laleh N and Azgomi M A. A Taxonomy of Frauds and Fraud Detection Techniques. In Prasad S K, Routray S, Khurana R, and Sahni S, editors, *Information Systems, Technology and Management*, pages 256–267, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[5] Farvaresh H and Sepehri M M. A Data Mining Framework for Detecting Subscription Fraud in Telecommunication. *Engineering Applications of Artificial Intelligence*, 24(1):182–194, 2011.

[6] Olszewski D. A Probabilistic Approach to Fraud Detection in Telecommunications. *Knowledge-Based Systems*, 26:246–258, 2012.

[7] Desai A B and Deshmukh R. Data Mining Techniques for Fraud Detection. *Int. Journal of Computer Science and Information Technologies (IJCST)*, 4(1):1–4, 2013.

[8] Saravanan P, Subramaniyaswamy V, Sivaramakrishnan N, Prakash M A, and Arunkumar T. Data Mining Approach For Subscription-Fraud Detection in Telecommunication Sector. *Contemporary Engineering Sciences*, 7(11):515–522, 2014.

[9] Akhter M I and Ahamad M G. Detecting Telecommunication Fraud using Neural Networks through Data Mining. *Int. Journal of Scientific & Engineering Research*, 3(3):1–5, Mac 2012.

[10] Awoyelu I, Adebomi A, Amoo A, Adebisi R, and Mabude C. Fraud Detection in Telecommunications Industry: Bridging the Gap with Random Rough Subspace Based Neural Network Ensemble Method. *Computer Engineering and Intelligent Systems*, 6(10):6–15, 2015.

[11] Mangala D and Kumari P. Corporate Fraud Prevention and Detection: Revisiting the Literature. *Journal of Commerce & Accounting Research*, 4(1):35–45, 2015.

[12] Hollmene J. *User Profiling and Classification for Fraud Detection in Mobile Communications Networks*. Ph.D Thesis, Department of Computer Science and Engineering, Helsinki University of Technology, 2000.

[13] Ogundile O O. Fraud Analysis in Nigeria’s Mobile Telecommunication Industry. *Int. Journal of Scientific and Research Publications*, 3(2):1–4, 2013.

[14] Sousa J V C. Telecommunication Fraud Detection Using Data Mining techniques. M.Sc. Thesis, Electrical and Computers Engineering, University of Porto, Portugal, Jun 2014.

[15] Ibrahim I A, Mohammed I B, and Saidu B. Fraud Management System in Detecting Fraud in Cellular Telephone Networks. *Int. Journal of Innovative Research in Computer Science and Technology (IJIRCST)*, 3(3):92–99, May 2015.

[16] Estevez P A, Held C M, and Perez C A. Subscription Fraud Prevention in Telecommunications using Fuzzy Rules and Neural Networks. *Expert Systems with Applications*, 31(2):337–344, 2006.

[17] Kou Y, Lu C T, Sirwongwattana S, and Huang Y P. Survey of Fraud Detection Techniques. In *Int. Conf. on Networking, Sensing and Control*, volume 2, pages 749–754, 2004.

[18] Wiens A, Wiens T, and Massoth M. A new Unsupervised User Profiling Approach for Detecting Toll Fraud in VoIP Networks. In *10th Advanced Int. Conf. on Telecommunications (AICT2014)*, pages 63–69, Jan 2014.
[19] Singh P and Singh M. Fraud Detection by Monitoring Customer Behaviour and Activities. *Int. Journal of Computer Applications*, 111(11):23–32, Feb 2015.

[20] Chandola V, Banerjee A, and Kumar V. Anomaly Detection: A Survey. *ACM Computer Survey*, 41(3):15:1–15:58, Jul 2009.

[21] Leite R A, Gschwandtner T, Miksch S, Gstrein E, and Kuntner J. Visual Analytics for Event Detection: Focusing on Fraud. *Visual Informatics*, 2(4):198 – 212, 2018.

[22] Dilla W N and Raschke R L. Data Visualization for Fraud Detection: Practice Implications and a Call for Future Research. *Int. Journal of Accounting Information Systems*, 16:1 – 22, 2015.

[23] Kranacher M J, Riley R, and Wells J T. *Forensic Accounting and Fraud Examination*. John Wiley and Sons, Hoboken, 2011.

[24] Steve Albrecht W, Albrecht C O, Albrecht C C, and Zimbelman M F. *Fraud Examination*. South-Western College Pub, 2011.

[25] Deloitte. Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse, Aug 2012. https://www.slideshare.net/DeloitteForensicCenter/visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016.

[26] Clopton J, Heitger L E, and Morrow L. Adding 'Augmented Intelligence' and 'Data Visualization' to the Mix, Nov/Dec 2014. https://www.fraudmagazine.com/article.aspx?id=4294985259.

[27] Kielman J, Thomas J, and May R. Foundations and Frontiers in Visual Analytics. *Information Visualization*, 8(4):239–246, December 2009.

[28] Keim D A, Mansmann F, Schneidewind J, Thomas J and Ziegler H. *VisualAnalytics: Scope and Challenges*, pages 76 – 90. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[29] Leite R A, Gschwandtner T, Miksch S, Gstrein E, and Kuntner J. Visual Analytics for Fraud Detection and Monitoring. In *IEEE Conf. on Visual Analytics Science and Technology (VAST)*, pages 201–202, Oct 2015.

[30] Bolton R J and Hand D J. Statistical Fraud Detection: A Review. *Statistical Science*, 17(3):235–255, 2002.

[31] S ili A and B asi B D. Visualization of Text Streams: A Survey. In R. Setchi, I. Jordanov, R.J. Howlett, and L.C. Jain, editors, *Knowledge-Based and Intelligent Information and Engineering Systems*, pages 31 – 43, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[32] Phua C, Lee V, Smith-Miles K, and Gayler R. A Comprehensive Survey of Data Mining-based Fraud Detection Research. *Computing Research Repository (CoRR)*, abs/1009.6119:1–14, 2010.

[33] Ngai E W T, Hu Y, Wong Y H, ChenY, and Sun X. The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature. *Decision Support Systems*, 50(3):559 – 569, 2011.

[34] Sharma A and Panigrahi P K. A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *Int. Journal of Computer Applications*, 39(1):37 – 47, 2012.

[35] Sithic H L and Balasubramanian T. Survey of Insurance Fraud Detection Using Data Mining Techniques. *ArXiv*, abs/1309.0806, 2013.

[36] Dumas M, McGuffin M J, and Lemieux V L. Financevis.net : A Visual Survey of Financial Data Visualizations. 2014. http://maximedumas.ca/files/dumas-2014-FinanceVis.pdf.

[37] Ko S, Cho I, Afzal S, Yau C, Chae J, Malik A, Beck K, Jang Y, Ribarsky W, and Ebert D S. A Survey on Visual Analysis Approaches for Financial Data. *Computer Graphic Forum*, 35:599–617, 2016.

[38] K.C. Cox, S.G. Eick, and G.J. Wills. Visual Data Mining : Recognizing Telephone Calling Fraud. *Data Mining and Knowledge Discovery*, 1(2):225–231, 1997.
[39] Miksch S and Aigner W. A Matter of Time: Applying a Data-Users-Tasks Design Triangle to Visual Analytics of Time-Oriented Data. *Computers and Graphics*, 38:286 – 290, 2014.

[40] Aigner W, Miksch S, Schumann H, and Tominski C. *Visualization of Time-Oriented Data*. Springer Publishing Company, Incorporated, 1st edition, 2011.

[41] Fawcett T and Provost F. Adaptive Fraud Detection. *Data Mining and Knowledge Discovery*, 1(3):291–316, Sept 1997.

[42] Hollme n J and Tresp V. Call-based Fraud Detection in Mobile Communication Networks Using a Hierarchical Regime-Switching Model. In *Conf. on Advances in Neural Information Processing Systems II*, pages 889–895, 1999.

[43] Hilas C S and Sahalos J N. User Profiling for Fraud Detection in Telecommunication Networks. In *5th Int. Conf. in Technology and Automation*, pages 382–387, 2005.

[44] Becker R A, Volinsky C, and Wilks A. Fraud Detection in Telecommunications: History and Lessons Learned. *Journal Technometrics*, 52(1):20–33, 02 2010.

[45] Manunza L, Marseglia S, and Romano S P. Kerberos: A Real-Time Fraud Detection System for IMS-Enabled VoIP Networks. *Journal of Network and Computer Applications*, 80:22 – 34, 2017.

[46] Volodina E, Aziz A, Rathgeb E P, and T Hossfeld. Application of Visual Analysis to Detect and Analyze Patterns in VoIP Attack Traffic. In *IEEE Int. Conf. On Trust, Security And Privacy In Computing And Communications*, pages 260 – 268, April 2018.

[47] Bastian M, Heymann S, and Jacomy M. Gephi: An Open Source Software for Exploring and Manipulating Networks. *Int. Conf. on Web & Social Media*, 8:361–362, 01 2009.

[48] Jajoo A, Vishnupriya G S, and Niket B. Customer Profiling and Anomaly Detection in Telecommunication Industry. *Int. Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)*, 4(11):19292–19296, 2016.

[49] Hilas C S. Data Mining Approaches to Fraud Detection in Telecommunications. *2nd Pan-Hellenic Conf. on Electronics and Telecommunications PACET*, 12, 2012.

[50] Huang M L, Liang J, and Nguyen Q V. A Visualization Approach for Frauds Detection in Financial Market. *Int. Conf. Information Visualisation*, pages 197–202, 2009.

[51] Luell J. *Employee Fraud Detection Under Real World Conditions*. Dissertation, Faculty of Economics, University of Zurich, 2010.

[52] Sacha D, Stoffel A, Stoffel F, Kwon B C, Ellis G, and Keim D A. Knowledge Generation Model for Visual Analytics. 20(12):1604 – 1613, 2014.

[53] Endert A, Ribarsky W, Turkay C, Wong W, Nabney I, Blanco I D, and Rossi F. The State of the Art in Integrating Machine Learning into Visual Analytics. *Computer Graphics Forum*, 36(8):458 – 486, 2017.

[54] Krause J, Perer A, and Bertini E. INFUSE: Interactive Feature Selection for Predictive Modeling of High Dimentional Data. 20(12):1614 – 1623, 2014.