(iv) Mini Tab-15

Mini Tab-15 [130] is easy-to-use and provides versatile tool to perform data analysis and quality assessments under a variety of research and manufacturing settings for both student and scientist. Help is provided from the software by the help tool. Web-based Answers Knowledgebase that is quickly accessed through the Help menu and statistical resources. Minitab offers several instructor-lead courses and a free technical support line. It provides user-friendly design to create an intuitive interface for learning. Minitab 15 can run on Windows 2000, XP or Vista and it is available in several languages except English. We have used trial version of Mini Tab-15 in our research work for Outlier Analysis, Multiple Regression Analysis, Peer Group Analysis and various statistical tests like t-Test, ANOVA (Analysis of Variance) etc.
CHAPTER-2

LITERATURE REVIEW

2.1 Previous related work done in the direction of fraud detection

According to Barnett & Lewis (1994) [7] Novelty detection, or so-called outlier detection, is the identification of “novel” or “unknown” events that an expert system is not aware of during training or testing. Outliers may indicate abnormal running conditions and lead to significant performance degradation. An outlier is one that appears to obviously deviate from the others of the sample in which it occurs or an observation which appears to be inconsistent with the remainder of the dataset. Using stepwise-logistic models, Persons O.S (1995) [99] found that financial leverage, capital turnover, asset composition and firm size are significant factors associated with fraudulent financial reporting. Prediction results suggest that these models outperform a naive strategy of classifying all firms as non fraud firms for all levels of relative costs of type I and type II errors. The models also correctly identify a large percentage of fraud firms and misclassify a relatively small percentage of non fraud firms when realistic relative error costs are assumed. Using Neural Networks, Fanning, Cogger and Srivasatava (1995) [28] studied to determine manipulation of financial information. After this, later on they demonstrated that 8 out of 20 variables (Trade receivable/sales, trade receivables/total assets, inventory/sales, tangible assets/total assets, total
liabilities/equity, sales/total assets) have reasonable explanatory power in determining manipulation of financial information through changing the extent of the database which was used in their first study. Using Neural Network Technique, Burge and Shawe-Taylor (1996) [87] developed profiling the behavior of the mobile phone users. Using Unsupervised Feed-Forward Neural Networks, Barson et al.(1996) [8] studied the detection of fraud in mobile phone networks. Using Bayesian Networks for Classification, Ezawa and Norton(1996) [26] developed Advanced Pattern Recognition and Identification (APRI). APRI's key strength is its ability to efficiently select relevant variables and dependencies to build conditionally dependent models. APRI reads the data from secondary storage at most five times during the entire model-building process. This is in sharp contrast to other Bayesian network learning systems, whose complexity grows linearly or quadratically with the number of input variables. To evaluate APRI, they built four probability models: a fully independent model, a limited independent model, and two dependent models. They used data sets with four to six million records, representing 600 to 800 million bytes of data. One of the dependent models classified 37% of the uncollectible calls correctly, versus the 10% classified correctly by the fully independent model. Using Logit Regression Analysis Beasley (1996) [9] studied to predict the relation between board of director composition and financial statement fraud. Using probit and logit models, Hansen et al. (1996) [37] studied powerful generalized qualitative-response model, EGB2, to model and predict management fraud based on a set
of data developed by an international public accounting firm. EGB2 specification easily accommodates asymmetric costs of type I and type II errors. This is important for public accounting firms since failure to predict fraud when it is present (a type II error) is usually very costly to the firm in terms of litigation. The results demonstrate good predictive capability for both symmetric and asymmetric cost assumptions. Using Hybrid Intelligent System with Neural Network and Fuzzy Expert System, Pacheco et al. (1996) [96] studied to diagnose financial problems in companies. Using Rule-based methods, Fawcett and Provost (1997) [29] studied that fraud detection process may be concerned with user’s profiling efforts in mobile telecommunication services to understand the behavior of customers to enable provisioning in the services to improve charging operations. Using Neural Networks Green and Choi (1997) [35] studied to develop a neural network fraud classification model employing endogenous financial data in corporate fraud. Using Fuzzy Logic, Deshmukh, Romine and Siegel (1997) [21] studied to provide a fuzzy sets model to assess the risk of managerial fraud. Using Expert System Eining, Jones and Loebbecke (1997) [25] studied to build an expert system applying the Logit statistical model to enhance user engagement and increase reliance on the aid. Using Neural Networks Fanning and Cogger (1998) [27] studied to use Neural Networks to develop a model for detecting managerial fraud. Using Logit Regression Analysis Summer and Sweeney (1998) [115] studied to investigate the relationship between insider trading and fraud. Using Rule-Based Fuzzy Reasoning System
Deshmukh and Talluru (1998) [20] studied to build a rule-based fuzzy reasoning system to assess the risk of managerial fraud. Using Feed Forward Neural Networks, Supervised Learning; Density Estimation with Gaussian Model and Bayesian Networks, Taniguchi et al. (1998) [117] developed CDR (Call Detail Record) extraction process, the detection is based on feature variables derived from call detail records. The unit of aggregation in time is one day. The feature mapping transforms the transactional data ordered in time to static variables residing in feature space. The used features reflect the daily usage of an account. Number of calls and summed length of calls to describe the daily usage of a mobile phone are used. National and international calls are regarded as different categories. Calls made during business hours, evening hours and night hours are also separated to sub-categories. From these categories they tried to define a model which will output the risk level of the subscriber in order to prevent misusage of the system. Using Evolutionary Algorithms (Genetic Algorithms) Welch, Reeves and Welch (1998) [120] studied to use genetic algorithms to aid the decisions of Defense Contractor Audit Agency (DCAA) auditors when they are estimating the likelihood of contracts fraud. Knorr E. and Ng. R. (1998) [71] studied finding of outliers (exceptions) in large, multidimensional datasets. The identification of outliers can lead to the discovery of truly unexpected knowledge in areas such as electronic commerce, credit card fraud, and even the analysis of performance statistics of professional athletes. According to them existing methods for finding outliers in large datasets can only deal efficiently with two
dimensions/attributes of a dataset. They studied the notion of DB-(Distance-Based) outliers. While they provided formal and empirical evidence of showing the usefulness of DB-outliers, they focused on the development of algorithms for computing such outliers. Using Rule-Discovery Methodology Roset et al (1999) [104] studied that standard classification and rule generation were not appropriate for fraud detection. The generation and selection of a rule set should combine both user-level and behavior-level attributes. Using Neural Networks, Cerullo and Cerullo (1999) [13] studied to predict the occurrence of corporate fraud at the management level. Using Neural Networks, Koskivaara (2000) [72] studied and investigated the impact of various pre-processing models on the forecast capability of neural network for auditing financial accounts. Using Neural Networks, Feroz et al (2000) [30] studied and predicted the possible fraudsters and accounting manipulations. Using Statistical Regression Analysis, Abbot, Park and Parker (2000) [1] studied and examined if the existence of an independent audit committee mitigates the likelihood of fraud. Using Logistic Model, Bell and Carcello (2000) [10] developed a model to estimate fraudulent financial reporting for an audit client. This model was based on the presence or absence of several fraud-risk factors. The fraud risk factors were identified in the final model which included weak internal control system, rapid company growth, inadequate or inconsistent relative profitability, management that just want to achieve earnings projections anyhow while lying to the auditors or is overly evasive, company ownership status (public vs. private), and interaction term
between a weak control environment and an aggressive management attitude towards financial reporting. Using Fuzzy Logic, Ammar, Wright and Selden (2000) [4] studied to use fuzzy set theory to represent imprecision in evaluated information and judgments. According to Aggarwal and Yu (2001) [2] outliers may be considered as noisy points lying outside a set of defined clusters or may be defined as points that lie outside of the set of clusters but are also different from the noise. Using Peer Group Analysis, Bolton & Hand (2001) [103] studied that the analysis of the time evolution of a given object (the target) relative to other objects that have been identified as initially similar to the target in some sense (the peer group). The objective of PGA is to characterize the expected pattern of behavior around the target sequence in terms of the behavior of similar objects, and then to detect any difference in evolution between the expected pattern and the target. Peer Group Analysis can be useful in detecting observations that deviate from their peers. This is useful in flagging anomalies, in areas such as fraud detection, fault detection, and behavior change detection. PGA tool in an unsupervised problem over real stock market data sets with continuous values over regular time intervals. Bolton, Hand and David J.H (2001) [11] studied that Credit Card Fraud falls broadly into two categories: (i) Behavioral Fraud and (ii) Application Fraud. They told that Application Fraud occurs when individuals obtain new credit cards from issuing companies using false personal information and then spend as much as possible in a short space of time. However, most credit card fraud is behavioral and occurs when details of legitimate cards have been obtained
fraudulently and sales are made on a 'Cardholder Not Present' basis. These sales include telephone sales and e-commerce transactions where only the card details are required. They concerned with detecting Behavioral Fraud through the analysis of longitudinal data. These data usually consist of credit card transactions over time, but can include other variables, both static and longitudinal. Statistical methods for fraud detection are often classification (supervised) methods that discriminate between known fraudulent and non-fraudulent transactions; however, these methods rely on accurate identification of fraudulent transactions in historical databases - information that is often in short supply or non-existent. They were particularly interested in unsupervised methods that do not use this information but instead detect changes in behavior or unusual transactions. They discussed two methods for unsupervised fraud detection in credit data in this paper and applied them to some real data sets. Peer group analysis is a new tool for monitoring behavior over time in data mining situations. In particular, the tool detects individual accounts that begin to behave in a way distinct from accounts to which they had previously been similar. Each account is selected as a target account and is compared with all other accounts in the database. Using Unsupervised Learning with Neural Networks, Burge and Shawe-Taylor (2001) [12] developed a Neural Network Technique for profiling the behavior of the mobile phone users. Using Logistic Regression, Spathis (2002) [113] studied and examined published data and develop a model to detect the factors associated with Financial Fraud Detection. Using Game Theory, Liu and Li
suggested a approach for prediction of attacks on Intrusion Detection System (IDS) protected systems and a given a specific prediction model for credit card fraud. Using Logistic Regression Spathis, Doumpos and Zopounidis (2002) [114] proposed that statistical techniques like logistic regression may be suitable for developing a model for identifying factors which are related to fraudulent financial statement. Non-parametric regression-based framework was used to run the falsified financial statement detection model. The proposed model was compared with discriminant analysis and logit regression methods for benchmarking. Using Logistic Regression Models, Owusu-Ansah et al. (2002) [91] explored the model to detect corporate fraud in New Zealand. Yu, Sheikholeslami and Zhang (2002) [137] presented a new method in which they applied signal-processing techniques to solve important problems in data mining. They introduced a novel deviation (or outlier) detection approach, termed FindOut, based on wavelet transform. The main idea in FindOut is to remove the clusters from the original data and then identify the outliers. Using Machine Learning, Maes, S et. al (2002) [82] studied and discussed about automated credit card fraud detection. They applied two machine learning techniques suited for reasoning under uncertainty-(i) Artificial Neural Networks and (ii) Bayesian Belief networks to the problem and showed their significant results on real world financial data. Using Fuzzy Neural Network and Logistic Model, Lin, Hwang and Becker (2003) [78] evaluated the utility of an integrated fuzzy neural network model for corporate fraud detection. Using Support Vector
Machine, Dong et al. (2004) [22] developed a Feature Extraction Method for Fraud Detection in Mobile Communication Networks. Using Finite Mixtures with Discounting Learning Algorithms, Yamanishi et al. (2004) [135] studied On-Line Unsupervised Outlier Detection. Using Fuzzy Logic and Expert Reasoning, Lenard and Alam (2004) [75] developed a model to develop clusters for different statements representing red flags in the detection of fraud. Using Game Theory and Strategic Reasoning Concepts, Wilks and Zimbelman (2004) [116] studied the detection and prevention of fraudulent financial reporting. They reviewed theoretical and empirical research from game theory, social psychology, judgment and decision making, and auditing to identify improvements in audit practice and promising areas for future research. This review focuses on the strategic fraud setting and suggests modifications in auditing standards that should facilitate auditors' use of strategic reasoning in this setting. They emphasized on three critical audit tasks—fraud risk assessment, audit planning, and audit plan implementation—and recommended changes to current auditing standards and identified potential research questions for each task. Hodge and Austin (2004) [39] reviewed some fundamental approaches to solve the problem of Outlier Detection. This technique is usually named as Novelty Detection since it aims to define the boundary of normality instead of estimating the density of the dataset. Using Support Vector Machine (SVM) and Artificial Neural Network (ANN) models, Wun-Hwa et al. (2005) [121] studied applications of SVM and ANN for Intrusion Detection. Using Fuzzy Logic and Expert System,
Pathak, Vidyarthi and Summers (2005) [97] studied for auditors to detect elements of fraud in settled insurance claims. Using Genetic Algorithm, Kiehl, Hoogs and LaComb (2005) [69] studied for automatically detection of financial statement fraud. Using Decision Trees, Neural Networks, Bayesian Belief Network and K-Nearest Neighbour, Kotsiantis et al.(2006) [73] studied to apply a hybrid decision support system using stacking variant methodology to detect fraudulent financial statements. Using Regression Analysis, Logit Model, Xuemin Huang(2006) [58] studied to analyze financial indexes which can predict financial fraud. Using Logistic Analysis and Clustering Analysis Haisong Ren (2006) [102] studied to establish a detecting model of fraud which can be used for empirical analysis of financial indexes. Using Fuzzy Logic Chai, Hoogs and Verschueren (2006) [14] studied to convert binary classification rules learned from a genetic Algorithm to a fuzzy score for financial data fraud rule matching. Allen, Litov and Mei (2006) [31] studied that corners were prevalent in the nineteenth and early twentieth century. They first developed a rational expectations model of corners and showed that they can arise as the result of rational behavior. After that using a novel hand-collected data set they investigated that price and trading behavior around several well-known stock market and commodity corners which occurred between 1863 and 1980. They found strong evidence that large investors and corporate insiders possess market power that allowed them to manipulate prices. Manipulation leading to a market corner tends to increase market volatility and has an adverse price impact on other assets.
They also found that the presence of large investors makes it risky for would-be short sellers to trade against the mis-pricing. Therefore, regulators and exchanges need to be concerned about ensuring that corners do not take place since they are accompanied by severe price distortions. Using Peer Group Analysis in Time Series Financial Data, Zakia et al. (2006) [140] demonstrated the experimental results of PGA tool in an unsupervised problem over real stock market data sets with continuous values over regular time intervals. The visual evidences have been shown through graphical plots that Peer Group Analysis can be useful in detecting observations that deviate from their peers. They also applied t statistics to find the deviations effectively. Their aim was to proceed by incorporating other information, other than simply the quantity sold, into the outlier detection process (PGA) to increase the effectiveness of the fraud detection system. They told following cases of possible outliers have to be investigated:

• Identify buyer IDs whose buy quantity rise up suddenly.
• Identify seller/buyer IDs who suddenly starts a large volume of trade.
• Identify stock IDs if trade volume or trade quantity increases suspiciously.
• Identify stock IDs with sudden raise or fall in price or having same buyer and seller.

studied detection of financial statement fraud. Using Genetic Algorithm, Hoogs et al. (2007) [40] studied detection of financial statement fraud based on anomaly scores as a metrics for characterizing corporate financial behavior. Using Classification and Regression Trees (CART), Bai, Yen and Yang (2008) [6] studied characteristics of China's listed companies and introduced classification and regression trees to identify and predict the impact of fraudulent financial statements. Using Logistic Regression Models, Yuan et al.(2008) [138] studied and employed a logistic regression model to test the effects of manager compensation and market competition on financial fraud in public companies among listed companies in China. Using Supervised and Semi Supervised Classification, Juszczak et al.(2008) [66] detected Financial Statement Fraud. Kyle and Viswanathan (2008) [3] studied that it is difficult to define illegal trade based manipulation and to prosecute it. Using Clustering Based Techniques Chandola et al. (2009) [15] suggested that there can be 3 types of anomalies- (a) Point Anomalies (b) Contextual Anomalies and (c) Collective Anomalies. A point anomaly is an individual data instance which is identified as anomalous with respect to the rest of the data. A contextual anomaly occurs when a data instance is anomalous in a specific context. For example, a temperature of 35 ° F is considered normal in winter, but anomalous in summer. Collective anomaly occurs when a collection of related data instances is anomalous. Using Neural Networks, M Krambia-Kapardis et al. (2010) [68] studied to test the use of Artificial Neural Networks as a tool in fraud detection. Using Neural Network and Support Vector Machines
Ravisankar et al. (2011) [101] studied to identify companies that resort to financial statement fraud. Using Neural Networks and Support Vector Machines, Perols (2011) [98] compared the performance of popular statistical and machine learning models in detecting financial statement fraud. Using Neural Networks and Bayesian Networks, Zhou and Kapoor (2011) [141] studied to detect financial statement fraud with exploring a self-adaptive framework (based on a response surface model) with domain knowledge. Bhattacharya and Marshall (2012) [119] used a sample of all top management who were indicted for illegal insider trading in the United States for trades during the period 1989-2002. They explored the economic rationality of this white-collar crime and found that indictments are concentrated in the “richer” strata after they control for firm characteristics like size, industry and growth opportunities, executive age, control for the opportunities available for illegal insider trading and control for the possibility that the regulators target the “richer” strata. Shu-Hsien Liao, Pei-Hui Chu and Pei-Yuan Hsiao(2012) [111] included survey of literature and the classification of articles from 2000 to 2011 in their research review and used Keyword indices and article abstracts to identify 216 articles concerning Data Mining Techniques applications from 159 academic journals (retrieved from five online databases). They surveyed and classified Data Mining Techniques with respect to the following three areas: (i) Knowledge Types (ii) Analysis Types and (iii) Architecture Types, together with their applications in different research and practical domains. They suggested that different social science
methodologies, such as psychology, cognitive science and human behavior might use Data Mining Techniques as an alternative methodology. Using Peer Group Analysis Y. Kim et. al. (2012) [134], proposed a method to detect suspicious patterns of stock price manipulation. This technique detects abnormal behavior of a target by comparing it with its peer group and measuring the deviation of its behavior from that of its peers. They proposed a method to improve the general peer group analysis by incorporating the weight of peer group members into summarizing their behavior, along with the consideration of parameter updates over time. Using real time series data of Korean stock market, they showed the advantage of the peer group analysis in detecting abnormal stock price change.

2.2 Types of Frauds

Black’s Law dictionary [52] defines the types of fraud that are as follows-

(a) Actual Fraud- A concealment or false misrepresentation through a statement or conduct that injuries another who relies on it in acting.

(b) Bank Fraud- The criminal offense of knowingly executing, or attempting to execute, a scheme or artifice to defraud a financial institution, or to obtain property owned by or under the control of a financial institution, by means of false or fraudulent pretense, representations or promises.
(c) **Bankruptcy Fraud**- A fraudulent act connected to a bankruptcy case; esp., any of several proscribed acts performed knowingly and fraudulently in a bankruptcy case, such as concealing assts or destroying, withholding, or falsifying documents in an effort to defeat bankruptcy-code provisions.

(d) **Criminal Fraud**- Fraud that has been made illegal by statue and that subjects the offender to criminal penalties such as fines and imprisonment.

(e) **Fraudulent Act**- Conduct involving bad faith, dishonesty, a lack of integrity or moral turpitude.

According to E.W.T Ngai et al. (2011) [24], Financial Fraud can be classified into following categories-

![Figure 2.2.1- Types of Financial Fraud](image-url)
Bank Fraud includes Credit Card, Money Laundering, Mortgage etc. Frauds. Insurance Fraud includes Automobile, Crop, Healthcare Insurance etc. Frauds. Securities and Commodities Fraud includes Market Manipulation, High Yield Investment, Hedge Fund, Commodities, Foreign Exchange, Brokers, Trading etc. Frauds. Other Related Financial Frauds includes Mass Marketing, Corporate etc. Frauds.

As our research work is mainly focused on Security Fraud Detection, so we have given detailed description of Security Fraud which is as follows-

2.3 Securities Fraud

According to Zakia et al. (2006) [140], Securities fraud usually takes place when brokers try to manipulate their customers into trading stocks without regard for the customers' own real interests. Stock fraud can be at a company level, or can be committed by a single stockbroker. Stock fraud can also vary in size from multi-million deals to penny stocks, but it consistently involves the intentional disregard for the financial situation of the customers and with personal profits. Corporate insiders, brokers, underwriters, large shareholders and market makers are likely to be manipulators.

2.3.1 Types of Securities Fraud

Following are the types of various securities frauds [42,46,49,50,52,54,92,124-127,133]:-

(a) Churning or Excessive Trading- Excessive trading in a customer's account to give profit to the broker/dealer in disregard of the

(b) **Unsuitable Investments** - Investments that ask the client to assume a greater financial risk than he or she can reasonably sustain; investments that are inconsistent with the client's financial needs; or investments in which the client is not adequately made aware of the risks involved.

(c) **Insider Trading** - Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information.

**Types of Insider Trading**

(i) **Front-Running** - When a broker/dealer, knowing a client has a large or market-sensitive order, puts through a transaction on his/her or another client's behalf, thus benefiting from the pre-warning. Can occur in either the securities or related instruments market. Financial firms may exploit institutional, corporate or other wholesale clients by executing proprietary trades in advance of client trades that may move the market.
(ii) **Scalping** - Trading prior to the release of a research report.

(iii) **Piggy-Backing** - When a broker, after observing a series of transactions of a client who has a high degree of success, repeats their investments for him/herself or clients, is similar to front-running but occurs after the transaction of the client has been completed.

(iv) **Inside Market Information** - When a broker/dealer disseminates information that certain trading activity is occurring or about to occur which will cause a price change. Similar to front running.

(v) **Classic Insider Trading** - When a director or associate of a company buys or sells shares before the release of a price-sensitive announcement.

(d) **Unauthorized Trades**-Unless the client of a brokerage firm has signed a contract that allows his or her broker to engage in discretionary trading, each transaction performed by the broker must be done with the client's permission.

(e) **Misrepresentation And False Statements**- Disguises risk factors associated with that particular stock; the broker intentionally misleads the customer about material facts regarding the stock.

(f) **Breach of Fiduciary Duty**- A breach of fiduciary duty includes, among other things, abdication of duty, abuse of trust and approval of
unlawful transactions, and may be based on nonfeasance as well as misfeasance.

(g) Over Concentration- Diversification is one of the most important rules of investing. Brokers should never concentrate all of a client's investments in one area. The broker who does so is potentially liable if that investment declines in value.

2.4 Market Manipulation

Most forms of market manipulation involve gaining control of the market by purchasing significant volumes at artificially set prices. Also called "Cornering". This can be followed by increasing or decreasing prices to desired levels. The more illiquid the stock, the easier to gain control and therefore the easier to manipulate.

2.4.1 Types of Market Manipulation

Following are the types of Market Manipulations [42,46,49,50,52,54,92,124-127,133]:-

(a) Demand Side Manipulation - Any manipulative technique used to increase the price of the securities. The rising price often leads other buyers into the market. The resultant market price bears no relation to the merits of the investment.
(b) **Supply Side Manipulation** - Any manipulative technique used to decrease the price of securities. The falling price induces others to sell, including short sellers. The resultant market price bears no relation to the merits of the investment.

### 2.4.2 Manipulative Acts in Stock Market

Following are the Manipulative Acts in Stock Market:

[42,46,49,50,52,54,92,124-127,133].-

(a) **Equities by Price**

(i) **Bait and Switch** - Stock-of-the-month recommendations are issued, usually without appropriate foundation, and sold to a group of customers. They then re-sell the stock for a small profit, thereby creating interest and encouraging other investors to buy at higher levels. This process can be repeated several times, pushing the price higher.

(ii) **Hype and Dump** - Talking up the price of stock by using false or exaggerated reports, rumours, brokers recommendations etc. Once price has risen, stock is dumped. The antithesis can be known as slur and slurp and occurs when the price of a stock is talked down, allowing manipulator to buy shares at lower prices.

(iii) **Pump and Dump** - Transactions at successively higher prices, giving the appearance of real activity by investors, then dumping or
selling at highs. Can occur as a supply side manipulation as well, by making undisclosed offers for only small parcels of shares, thereby inducing others to sell and allowing the manipulator to buy a large parcel of shares later at a cheaper price.

(iv) **Ramping**- Marking (up) the close either by placing bid or purchasing parcel at or near the close which changes the closing price (bid often dropped next morning). Also called painting the tape or window dressing. Can also be used to push share price lower.

(v) **Window Dressing**- Ramping by institutional investors to allow valuation at desired prices.

(b) **Equities by Volume**

(i) **Chain Letter Rally**- Occurs as speculators enter market thereby unwittingly assisting manipulator by increasing volume and price movement.

(ii) **Churning**- The manipulator acquires a holding of shares and then places both buy and sell orders either through one broker or several in order to create an impression of large turnover. These orders are usually placed at progressively higher prices, also called pass the parcel.

(iii) **Pools**- A group of manipulators who trade shares back and forth between themselves, usually through one broker, thereby raising
volumes and creating other investor interest. Similar to churning and pass the parcel.

(iv) **Short Squeeze**- Purchasing significant amount of stock i.e. cornering the market in order to force short sellers to purchase shares to cover their short positions at successively higher prices, thereby increasing the price.

(v) **Matched Orders**- Pre-arranged trades by associated parties who enter purchase or sale order knowing associate has entered corresponding order.

(vi) **Wash Sales**- Purchase and sale orders placed at same time where beneficial ownership does not change.

(c) **Options**

   (i) **Capping and Pegging**- When the holder of a large short put and/or call option position sells or buys the underlying security in order to affect the price of the security so that the option position expires valueless and the holder avoids assignment.

   (ii) **Mini-Manipulation**- A relatively short-term stock manipulation in which the price of an underlying stock is manipulated upwards or downwards in order to benefit the liquidation of an open option position.

   (iii) **Short Squeeze Inter Market**- A short squeeze between the share market and a related security, such as the options market.