ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 3, March 2015*

# Deportation of Market Manipulation using ADS

**Vaishali Ingale[1], Mohnish Chaudhary[2], Rashmi Sharma[3] , Ravinder Kumar[4], Vaishnavi Pimpalnerkar[5]**

Professor, Information Technology, Army Institute of Technology, Pune, India [1]

Student, Information Technology, Army Institute of Technology, Pune, India[2,3,4,5]

**Abstract:** Market manipulation remains the biggest concern of clients in today's securities market, despite fast and strict responses from regulators and exchanges to market participants that pursue such practices. The existing methods in the industry for detecting fraudulent activities in securities market rely heavily on a set of rules based on expert knowledge. In this paper we use authenticated data structure(ADS) to ensure integrity of data. By use of authenticated data structures, we can prevent this market manipulation done on the cloud in the form of stock bashing, pump and dump and runs etc. Solution to prevent clients buyers from this fraud or false information is that the server need to give a digest , proof of the information along with query answer to the client. And the client on the other hand can verify the information to be legitimate or not by the help of query, digest, proof, public key.

**Key words**: Market manipulation, ADS, Cloud, Client.

## I. INTRODUCTION

Market manipulation is the act of artificially inflating or deflating the price of a security. In most cases, manipulation is illegal[1]. It is much easier to manipulate the share price of smaller companies, such as penny stocks, because they are not as closely watched by analysts as the medium- and large-sized firms.


Figure- Three party model for ADS

In a stock exchange market, stock buyers and sellers makedeals based on the changing price. To identify stock market trends, stock buyers may frequently consult exchange providers about historical and real-time stock prices. With a large number of stocks, the footprint of the stock price data would easily grow out of a regular company's computing capability or its IT budget. Moreover, as there are more and more stock brokers in the market, it requires huge computing power to serve such a large customer base data outsourcing causes issues of trust, because the cloud, being operated by a third-party entity, is not fully trustworthy. A cloud company could deliver incomplete query results to save computation cost or even maliciously manipulate data for financial incentives, e.g., to gain an unfair advantage by colluding with a data user competing with the rest. Therefore, it is imperative for a data owner to protect data authenticity and freshness when outsourcing its data to a third-party cloud. It is crucial to assure *temporal freshness* of data, i.e., obtain proofs that the server does not omit the latest data nor return out-of-date data. Especially when the value of the data is subject to continuous updates, it is not sufficient to guarantee only the *correctness* of data because a data sclient1 expects to obtain the "freshest" data. For example, a data user can query the latest price of a stock, the latest bid towards the purchase of a product in an auction, or the sensor readings of any monitored attributes at a specific time.

## II. TYPES OF MANIPULATION

**Pump and dump:**

This scheme usually involves usage of false and deceptive statements in order to hype stock so ,Cthat cheaply purchased stock can be selled at much higher price.Once the operators of the scheme"dump" their overvalued shares, the price falls and investors loose their money.These schemes involves telemarketing and internet fraud.

**Quote Stuffing:**

In this high frequency traders tactically enter and withdraw from the market, to flood the market. This creates confusion in the market. The price quote get delayed while stuffing is occurring simply by placing and cancelling orders at a rate that corporeally exceeds the bandwith of market data feed lines. The orders pile up in buffers, and the delay lasts until the buffer drains.

**Front Running:**

It is an illegal practice where the broker buys the shares at cheaper rate and sells the customer by putting his or her


DOI 10.17148/IJARCCE.2015.43152

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 3, March 2015*

own financial interest above the customers interest. For example,auppose a broker receives a market order from a customer to buy a large block-say,10,000 shares-of some stock,but before placing the order for the customer, the broker buys 5,000 shares of the same stock for his own account at $100 per share, then afterward places the customer's order for 10,000 shares, driving the price upto $102 per share and allowing the broker to immediately sell his shares for, say, $101.75, generating a significant profit of 2,500 in just a short time.This $2,500 is likely to be just a part of the additional cost to the customer's purchase caused by the broker's self dealing.

**Churning:**

In churning excessive trading is done on clients accounts in order to generate commissions.For example, for an actively traded mutual fund,the entire assets of the fund will be involved in buying and selling transactions once every six to twenty-four months. In churning cases it is done once a month, or even more frequently.

**Wash Trading:**

In wash trading, same client is refrenced on both sides of the trade i.e buying shares of a company from one broker and selling them to different broker It creates misleading appearance of an active interest in a stock.

**Ramping:**

A significant increase in the level of output of a company's products or services. A ramp up typically occurs in anticipation of an imminent increase in demand. While it is generally a feature of smaller companies at an early stage of development, a ramp up can also be undertaken by large companies that are rolling out new products or expanding in new geographies.

## III. RELATED WORK

The existing approach in industry for detecting market manipulation is a top-down approach that is based on a set of known patterns and predefined thresholds. Market data such as price and volume of securities (i.e. the number of shares or contracts that are traded in a security) are monitored using a set of rules and red flags trigger notifications. Then, transactions that are associated with the detected periods are investigated further as they might be associated with fraudulent activities. These methods are based on expert knowledge but suffer from two issues i) detecting abnormal periods that are not associated with known symptoms (i.e. unknown manipulative schemes), ii) adapting to the changing market conditions whilst the amount of transactional data is exponentially increasing (this is due to the rapid increase in the number of investors and listed securities) which makes designing new rules and monitoring the vast data challenging[2]. Data mining methods may be used as a bottom-up approach to detect market manipulation based on modeling historical data. These models can be used to identify market manipulation on a new dataset without relying on expert knowledge. The initial results of such models in the literature are encouraging. However, there are many challenges involved in developing data mining methods for detecting fraudulent activities and market manipulation in securities market including heterogeneous data (different forms such as news data (e.g. Factiva3 ), analytical data (Trade And Quote (TAQ) from exchanges) and fundamental data (e.g. COMPUSTAT4 )), unlabeled data (labeled data is very rare because (a) it is very costly and typically requires investigation by auditors, (b) the number of positive samples (fraud cases) constitute a tiny percentage of the total number of samples (also known as imbalanced classes)), massive datasets (NASDAQ stock exchange with over 2700 securities listed facilitates more than 5000 transactions per second using its trading platform SuperMontage. Another factor is High Frequency Trading - algorithms that could submit many orders in millisecond 5 ), performance measures and complexity. The problem of detecting market manipulation in securities market is a big data problem where rapidly increasing heterogeneous data from different sources and in different forms are integrated for training prediction models. The impacts on the market, privacy and the training of auditors are other issues that need to be addressed but are not in the scope of this paper.

## IV. OUR CONTRIBUTION

In this paper we are trying to save clients from market manipulations. Since most of the manipulation is done by the middle layer manipulators. So compare to exixting work we provide a solution to maintain authenticity and integrity of data.

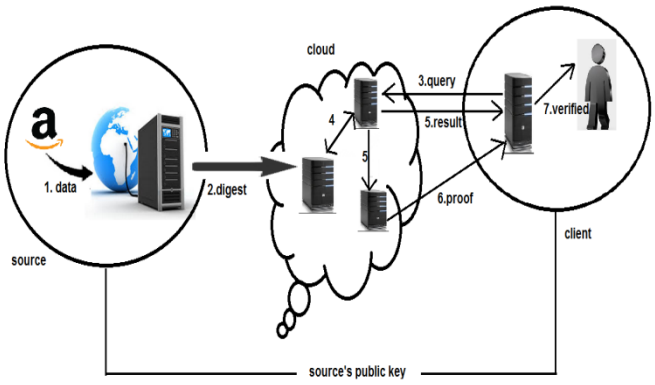


Fig-Stock exchange on cloud

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 3, March 2015*

Figure 1 illustrates our system model. In this ecosystem, there are three parties in different administrative domains:
• a data owner, e.g., a small technology start-up company
• a data user, e.g., a customer of the company
• a public cloud, offering data storage and management

Note that both the data owner and the data user do not fully trust a public cloud as it is operated by a third-party company with its own interests, partially conflicting with those of the small start-up company.

- In this scenario, the data owner outsources a key-value dataset to a public cloud, and each stream unit is an update to a key-value record in the dataset, submitted by the data owner to the public cloud.
- In order to provide data authenticity, a data owner employs a *signer* to sign the raw data stream before publishing it to a cloud (steps 1 and 2 ).
- The data user typically uses the Insert/Findinterface to access the key-value dataset. The data user issues Get queries to the outsourced keyvalue store in the public cloud.
- The usual query path returns a result of interests (steps 3 , 4 , and 5 ), and an additional verification path (steps 5' , 6' , and 7' ).
- A prover in a cloud composes a proof and delivers it to the data user's *verifier*, which verifies the authenticity of the query results for the data user. We assume that the data user knows the public key of the data owner, and that the signer and the verifier are time-synchronized (e.g., using a trusted network time services) for freshness authentication.

## V. CONCLUSION

The advancement in ADS is changing the horizon of security over the network and ultimately resulting in maintain the integrity of data. The use algorithm likes SHA1 and RSA are helpful for a secure transmission of data over the network like internet. There are tremendous opportunity to work here in this arena and to make contribution.

In this paper we have concluded that ads is a better technology to avoid market manipulations.Using ads we generate digest of a document.In digest original data cannot be manipulated and manipulations like pump and dump,wash trading etc we have studied in this paper can be avoided.

## ACKNOWLEDGEMENT

The authors are extremely thankful to Mrs. Vaishali Ingale, Dr. Sangeeta Jadhav and our college Army Institute of Technology for their valuable contribution and suggestions

## REFERENCES

[1] http://www.investopedia.com/terms/m/manipulation.asp
[2] Koosha Golmohammadi, Osmar R. Zaiane University of Alberta Department of Computing Science Edmonton, Canada {golmoham, zaiane}@ualberta.ca
[3] M. L. Huang, J. Liang, and Q. V. Nguyen, "A Visualization ApprDavid Díaz Universidad de Chile Departamento de Administración, Facultad de Economía y Negocios Santiago,Chile ddiaz@unegocios.cloach for Frauds Detection in Financial Market," in 2003 13th International Conference Information Visualisation, 2003, pp. 137–202.
[4] Z. Ferdousi and A. Maeda, "Unsupervised Outlier Detection in Time Series Data," in 22nd International Conference on Data Engineering Workshops (ICDEW'06), 2006, pp. x121–x121.
[5] M. Vlachos, K.-L. Wu, S.-K. Chen, and P. S. Yu, "Correlating burst events on streaming stock market data," Data Min. Knowl. Discov., vol. 16, no. 1, pp. 103–133, Mar. 2007.
[6] Yuzhe Tang† Ting Wang‡ Xin Hu‡ Jiyong Jang‡ Ling Liu† Peter Pietzuch♯ †*Georgia Institute of Technology, Atlanta GA, USA, Email:* {yztang@, lingliu@cc.}gatech.edu ‡*IBM Research Center, Yorktown Heights NY, USA, Email:* {tingwang, xinhu, jjang}@us.ibm.com ♯*Imperial College London, UK, Email:* prp@doc.ic.ac.uk