Deployment of Secure Data Parameters Between Stock Inverters and Interfaces Using Command-Contamination-Stealth Management System

Santosh Kumar Henge[1]*, Sanjeev Kumar Mandal[2], Ameya Madhukar Rane[3], Megha Sharma[4],
Ravleen Singh[5], S Anka Siva Phani Kumar[6], Anusha Marouthu[7]

Associate Professor, Department of Computer Science and Engineering, School of Computer Science and Artificial Intelligence,
SR University, Warangal, 506371, India[1]
Assistant Professor, Department of CS and IT, Jain (Deemed-to-be University), Bangalore, India[2]
Department of Finance, Regenesys Business School, Johannesburg, Santon, South Africa[3]
Associate Professor, Department of Finance, Thakur Institute of Management Studies and Research, Mumbai, India[4]
Assistant Professor, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, AP, India[5]
Assistant Professor, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, AP, India[6]
Associate Professor, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, AP, India[7]

***Abstract*—The security issues more impact on stock data which allows the stockholders (SHs) and stock-inverters (SIs) to predict and invert false assets and stock values. Because of the security flaws and threads that let an attacker take over network devices, the attacker uses the system to attack another system. These problems have an even greater influence on stock data, which gives stockholders (SHs) and stock-inverters (SIs) the ability to forecast and reverse fictitious assets and stock values. This study suggests test scenarios regulate different BOTNETs, layered threshold-influenced data security parameters, and DDoS vulnerabilities for stock data integration and validation. In order to study the behavioral entry and exit sites of SHs and SIs, it has integrated three-tiered procedures with threshold-impacted data security criteria and data matrices. Role Management (RM), Remote Level of Command Executions (RLCE), LAN-WAN-LAN Transmission (LWL-T), and Detection of Conceal and Prevention (DoCP) environments are the frameworks of the first layer. The RM, RLCE, LWL-T and DoCP are tuned with threshold-influenced data security parameters which are more influencing stock values. The second layer is framed with Module Management (MM), Command Module (ComM), Contamination Module (ConM), and Stealth Module (SM). The third layer is framed with expected scenarios and threshold of various vulnerabilities, a thread which occurs based on DoS and BOTNETs. All these layers are interconnected together and integrated with behavioral factors of SHs and SIs. The vulnerabilities are tuned with SHs and SIs input data, then filtered with SHs and SIs behavioral matrices, the alerts has been generated according to their existing entries of the data. These influenced threshold metrics tuned through ARIMA and LSTM for future analysis of stock values. The authentication mode has synchronized dual and multi authentication mode of execution, which tuned to cross verify the investors credentials.**

Keywords*—Robot-network (BOTNET); Module Management (MM); Role Management (RM); Detection Conceal and Prevention (DoCP); LAN-WAN-LAN transmission (LWL-T); Remote Level Command Executions (RLCE); Distributed Denial-of-Service (DDoS)

I. Introduction

The BOTNETs are a highly effective type of assault to seize the credentials of a completely distributed network. The cyber security experts are facing complex problems when they face the BOTNET attack on their localized secure networks which is completely controlled by the server. This research described the execution stages of BOTs and BOTNETs along with the attacking scenarios; and the precaution scenarios to prevent BOTs and NETBOTs from cybercriminals. The Distributed Denial-of-Service (DDoS) is a cyber-attack which operated by the assailant from the inaccessible systems. The assailant utilizes the system to assault a distinct system due to the security vulnerabilities and threads that allow an assailant to take control of the network devices. The presence of exceptionally slow network performance, the inaccessibility of a certain website, or the inability to access any website is sign of DoS or DDoS attack. a sharp rise in the volume of spam that will be received on a certain account; DDoS assaults are made to attack any component of a company and its resources, and they can quickly shut down a particular computer, service, or an entire network; target alarms, printers, phones, or laptops; attack system resources like bandwidth, disk space, processing time, or routing information; run malware that messes with CPUs and causes microcode faults in computers; To drain system resources and crash the operating system, exploit operating system flaws.

A DDoS botnet is a collection of compromised machines that are used to overwhelm servers or websites with excessive traffic, resulting in server crashes and unavailability. Malware from DDoS botnets is not always obvious or affects the device right away. Sometimes the virus takes over the device right away, while other times it operates in the background and stealthily carries out the attacker's commands [1]. The bot herder, also known as the botmaster, is in charge of the DDoS botnet and uses intermediary machines, or C&C servers, to remotely control the bots. They can communicate with the C&C servers via HTTP websites, IRC protocols, and well-known social media platforms like Facebook, Twitter, and Reddit. Peer-to-peer botnets, which are managed by one or more botmasters, can be created by botnet servers interacting with one another. DDoS assaults have a significant effect on numerous industries, including finance, technology, e-commerce, media and entertainment, healthcare, and many more. These industries are particularly vulnerable to DDoS assaults because of their vital role in the world economy and widespread usage of internet services. It will have a greater effect on the financial data consequences related to lost revenue. DDoS attacks have the potential to interfere with payment processing, stock trading, and internet banking. There may be large income losses as a result of the ensuing downtime [2]. Due to their low security and Internet connectivity, Internet of Things (IoT) devices pose a number of hazards, including the possibility of malware penetration and IoT botnet membership. Distributed Denial-of-Service (DDoS) assaults are among the many forms of large-scale attacks that are launched via the Internet of Things botnets [3].

LSTM makes exclusive use of elements known as gates. Stock market prices are non-stationary data inputs. Rising and falling movements [3] in the Intraday or Off-market are non-linear. Assessment of predicting stock prices can give evidence to be effective in an investor’s profession and growth [4]. These financial advisors are part of insider trading, and they make wrong use of investor emotions [5] and thus result in investor wealth deterioration or exploitation. All investigators aspire to efficiently original stock values with minimal noise so that stock purchasers may select when to trade or capitalize to attain sizable revenue [6]. Meanwhile, Stock prices are extremely volatile and arbitrary [7]. Altogether, that specifies no consistency in patterns of data for modeling stock prices over an efficient time interval. LSTMs mesh [8] are properly utilized on time series data for the assessment of classification, computing [9] and making predictions [10]. In other words, LSTM is also known for its memory storage capacity.

The security issues more impact on stock data which allows the stockholders (SHs) and stock-inverters (SIs) to predict and invert on false assets and stock values. This research has formulated with two major objectives: to design layered threshold influenced data security system with the secure parameters and test cases to control various BOTNETs, DDoS vulnerabilities for stock data validation and integration before stock investment; to create efficient forecast data stream conception for stockholders to practice in creation quick conclusions using several open-source repositories for raw mathematical data. The hypothesis study was conducted by several investigators using numerous recital indicators, and it can regulate whether the system would be implemented successfully or unsuccessfully in the future based on the gains or losses that distinct stock holders [11] experience over the course of their lifetimes [12]. Because LSTM can solve problems in the future, it was developed to get over issues that prevented RNN modeling's [13] execution. It is undeniable that the input gate activates whenever a new piece of data is incremented into the present state of the LSTM, and it can be used to clarify problems with long-term interdependence [14] of variables in RNNs. What gets erased from memory is decided by the output gate. Humans are unable to start thinking from scratch about every problem all the time [15]. Last but not least, MA is an acronym for moving average, which foresees the relationship between data and residual error [16].

The main objective of this research is to use a command-contamination-stealth management system to deploy secure data parameters between stock inverters and interfaces. For the integration and validation of stock data, this study proposes test scenarios to control various BOTNETs, layered threshold-influenced data security parameters, and DDoS vulnerabilities. It has combined three tiered procedures with threshold influenced data security standards and data matrices to examine the behavioral entry and exit sites of SHs and SIs.

The article has frame with five sections: Section II presents the related work, which expresses the background of the study. Section III includes the proposed secure stock market data integration using layered threshold based access control approach. The proposed methodology executed with two stages: the stage 1 composed with layered threshold influence data security system and stage 2 integrated the data security system based predication of stock values. Section IV includes the results and discussion; Section V contains the conclusions.

II. Related Work

The related work describes the existing models and methodologies which proposed to protect and secure the stock data passing through the secure distributed servers. Arnau Erola et.al proposed the detection of IT with the deployment of the CITD tool in 3- multinational organizations. This approach justified its implementation based on the CITD tool and the results achieved from employing the recognition system in real network infrastructure over six months [17]. A novel authentication technique for IAs was proposed by the author Rajamanickam, S., and it was based on the reliable cryptographic method ECC. The suggested protocol is not only resilient to insider attacks but also prevents several attacks, according to an informal security study of the protocol.

By focusing on its historical stock values, F. Kamalov, L. Smail, and I. Gurrib (2020) investigated various approaches to doing prediction based on neural networks for the impending market opening value of the SP 500 global indices [18]. In order to improve correctness, B. B. P. Maurya et al. used parameters such as E Ratio, Moving Average, and MACD [19] to explain the complexity of ML problems. For the purpose of intraday guidance, C.C. Emioma et al. announced their intention to use the least-squares LR model [20]. According to research by Nti IK et al., 66% of financial market investment decisions were based on technical analysis, and an additional 11% and 23% were long-term and anticipatory selections, respectively. In combined analyses, 8.26% and 2.46% were dependent [21]. Focusing on the Brazilian stock-market, Samara A. Alves et al. created a decision pattern to determine the stock value in relation to specific precise statistics [22]. By computing using the genetic programming method and classifying the stocks into groups that can be useful for investor decisions, Chun-Hao Chen et al. suggested an algorithm for company-based portfolios [23]. Adjustable Neuro because fuzzy inference systems struggle to handle huge inputs, the cost of computation increases dramatically when gradient learning and complicated structures are present. The location of the required membership function and the curse of dimensionality are two additional difficulties [24]. The author concluded that partially familiar nodes, linkages, and labels cannot be presented effectively in networks with incomplete knowledge, and their extensive effort is centered on building an inductive drive-in model to address real-world network issues. ANFIS constraint's relationship to computing cost is direct [25]. Early risk management strategies relied on fundamental corporate performance statistics based on specific quarters that suggested future expectations in a good direction but were not always accurate, resulting in significant financial losses [26-28].

Hybrid artificial intelligence systems, such the neural fuzzy logic control system [29] [30], neural genetic system, and genetic fuzzy systems, are used in modern safe systems, computer visions, and medicinal improvements. Author recommends the SP-MAACS scheme, a safe and privacy-preserving multi-authority access control system, for cloud-based healthcare data sharing [31]. The author in [32] provides a thorough analysis of the best techniques for securely exchanging and securing data in the cloud environment. The post-quantum mathematical cryptography and secure key data distribution used for the user-storage-transit-server authentication procedure. To secure data in user, server, transit, and storage modes, it provides technical solutions and security scenarios. To protect data privacy, the author [33] proposes a novel algorithm-based method that permits data sharing within a variety of chunk sizes for the position and differentially combines the chunked data with the MD5 value.

Author in [34] has developed a novel ABE system that protects user privacy when providing keys. The functionality of attribute auditing and key generating are separated in our new scheme to avoid the KGC from learning a user's attributes and the attribute auditing center (AAC) from gaining the user's secret key. Author in [35] proposed the accuracy of security scenario prediction, the initial prediction value is changed, and integrated time-varying weighted Markov chain is used for error prediction. With three main objectives in mind—a description of the causes and impact elements of insider attacks; implications of enterprise multi-tenancy with behavior rule-based design; and integration of behavior guidelines and security thresholds to regulate user accessibility and stop internal threats and attacks. The author in [36] proposes a revolutionary user-server authentication technique and key aggregate searchable encryption (KASE) technology KASE scheme that allows multi-delegation without TTP. Attribute-based encryption technology is a safe method that provides granular access control to the encrypted data writer [37-39] .The assailant utilizes the system to assault a distinct system due to the security vulnerabilities and threads allows an assailant take control of the network devices. These issues more impact on stock data which allows the stockholders (SHs) and stock-inverters (SIs) to predict and invert on false assets and stock values [40]. This research suggests test scenarios to regulate various BOTNETs, layered threshold-influenced data security settings, and DDoS vulnerabilities for stock data integration and validation.

III. Methodology

This study suggests test scenarios regulate different BOTNETs, layered threshold-influenced data security parameters, and DDoS vulnerabilities for stock data integration and validation. In order to study the behavioral entry and exit sites of SHs and SIs, it has integrated three-tiered procedures with threshold impacted data security criteria and data matrices

A. Command-Contamination-Stealth Management System-Based Three-Layered Security Framework

This research is proposing layered threshold influenced data security parameters, test cases to control various BOTNETs, DDoS vulnerabilities for stock data validation and integration. It has integrated three layered processes with threshold influenced data security parameters and data metrices to analyze SHs and SIs behavioral entry and exit points. Layered Threshold influence data security methodology parameters, test cases to control vulnerabilities for stock data validation and integration shown in the Fig. 1.

The first layer is framed with Role Management (RM), Remote level of Command Executions (RLCE), LAN-WAN-LAN Transmission (LWL-T), Detection of Conceal and Prevention (DoCP) environments. The RM, RLCE, LWL-T and DoCP are tuned with threshold influenced data security parameters such as SIs number or ID (SI-ID), name (SIN), nationality (SINA), location (SIL), synchronized A/C number (SACN), number of stocks invested (NSI), previous history (SIPH), SI introducer ID (SIID) and system credentials (SC) such as MAC, IP along with the authentication mode. The second layer has framed with Module Management (MM), Command Module (ComM), Contamination Module (ConM), Stealth Module (SM). The third layer framed with expected scenarios and threshold of various vulnerabilities, thread which occurs based on DoS and BOTNETs. In third layer, the DoS and BOTNETs based vulnerabilities analyzed using Open-VS analyzer and build alerting system which helps to generate alerts according to the vulnerability threshold values.

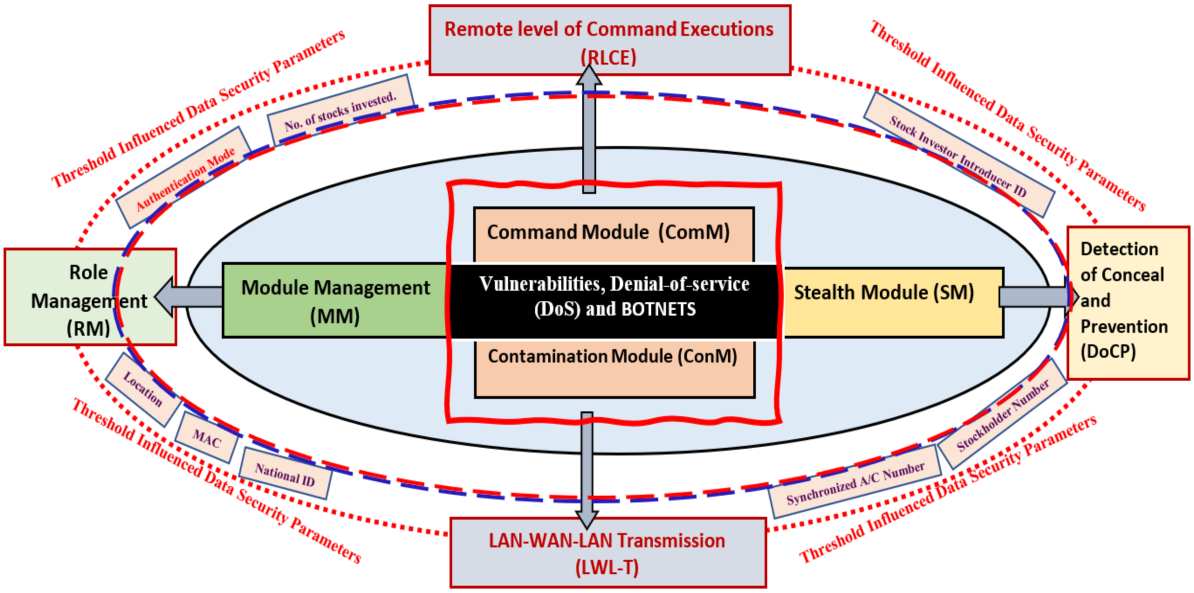
Remote level of Command Executions (RLCE)
Threshold Influenced Data Security Parameters
Threshold Influenced Data Security Parameters
No. of stocks invested.
Authentication Mode
Stock Investor Introducer ID
Command Module (ComM)
Vulnerabilities, Denial-of-service (DoS) and BOTNETS
Contamination Module (ConM)
Module Management (MM)
Stealth Module (SM)
Role Management (RM)
Detection of Conceal and Prevention (DoCP)
Location
MAC
National ID
Synchronized A/C Number
Stockholder Number
Threshold Influenced Data Security Parameters
Threshold Influenced Data Security Parameters
LAN-WAN-LAN Transmission (LWL-T)

Fig. 1. Layered threshold influence data security methodology parameters, test cases to control vulnerabilities for stock data validation and integration.

All these layers are interconnected together and integrated with behavioral factors of SHs and SIs. The vulnerabilities are tuned with SHs and SIs input data, then filtered with SHs and SIs behavioral matrices, the alerts has been generated according to their existing entries of the data as shown in Fig. 2.

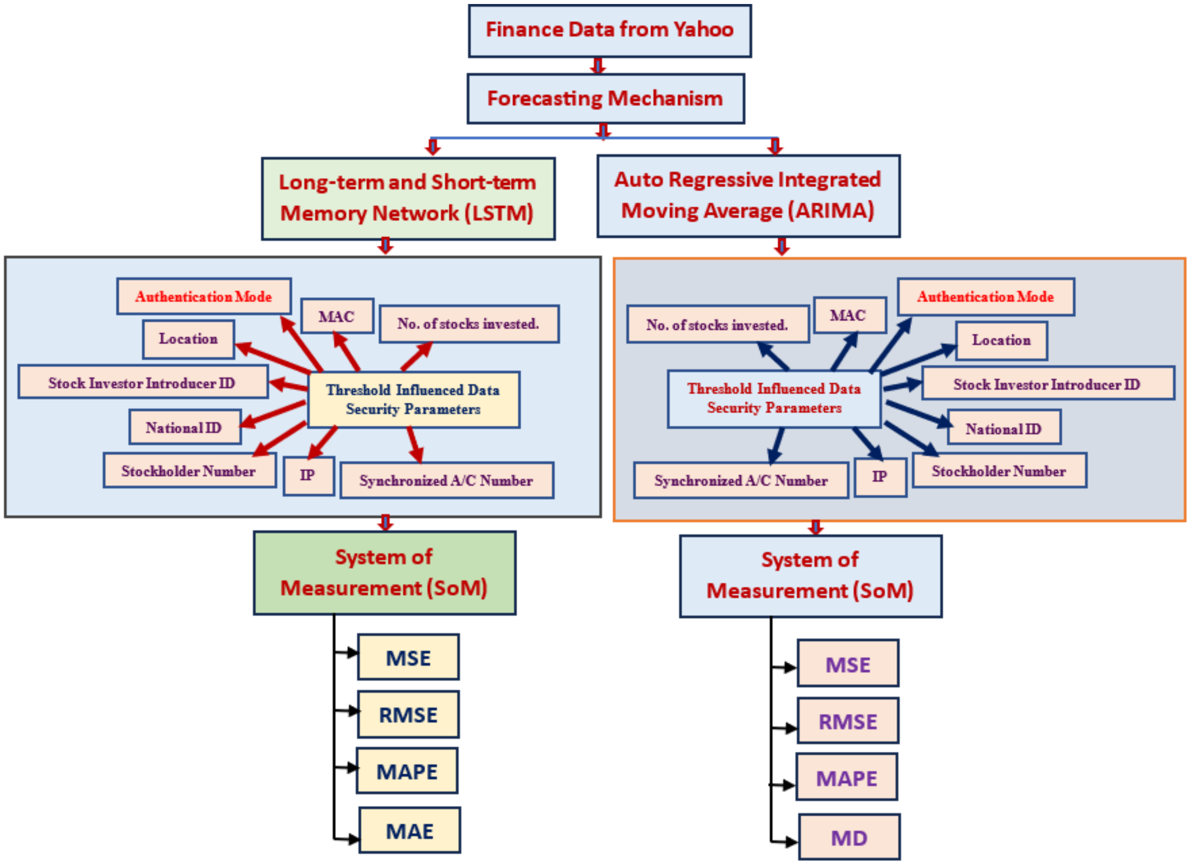
Finance Data from Yahoo
Forecasting Mechanism
Long-term and Short-term Memory Network (LSTM)
Auto Regressive Integrated Moving Average (ARIMA)
Authentication Mode
MAC
No. of stocks invested.
Location
Stock Investor Introducer ID
Threshold Influenced Data Security Parameters
National ID
Stockholder Number
IP
Synchronized A/C Number
No. of stocks invested.
MAC
Authentication Mode
Location
Threshold Influenced Data Security Parameters
Stock Investor Introducer ID
National ID
Synchronized A/C Number
IP
Stockholder Number
System of Measurement (SoM)
MSE
RMSE
MAPE
MAE
System of Measurement (SoM)
MSE
RMSE
MAPE
MD

Fig. 2. Integration of threshold influenced data security parameters on Saudi stock based on ARIMA and LSTM.

B. Implementation of the Security System and the Testing Scenarios

These influenced threshold metrices analyzed individually under the considerations of Auto Regressive Integrated Moving Average (ARIMA) and Long-term and Short-term Memory Network (LSTM), which helps to analyze the customer stock entries and values to avoid malware or thread-based entries. The authentication mode has synchronized dual and multi authentication modes of execution, which are tuned to cross-verify the investors credentials.

IV. Results and Discussion

Initially, the experimental setup has framed with two stages of execution scenarios. The stage1 representing the layered threshold influence data security system has built with the integration of three layers. The stage 2 representing the prediction scenario of stock values.

A. Stage 1: Layered Threshold Influence Data Security System

The layered threshold influence data security system has been built with the help of Red Hat enterprise Linux operation system with 21 client systems which is integrated with the Red Hat server and used the checkpoint console to analyze IN and OUT stack entries from-to SHs and SIs. The Open-VS application has integrated to analyze vulnerabilities, which has helped to prepare the test-cases with supporting filters.

B. Stage 2: Data Security System based Predication of Stock Values

LSTM, sequential, dense, and Panda's libraries should be imported first. Additionally, use the Yahoo Finance API to get the stock price and display the date in tabular format. Find out how many rows and columns the data set contains. Visualize the past closing price data during that time. Then, change the recently created Df into a NumPy array by adding a close column. Scale the data after figuring out how many rows to count in order to train the computer model. The x_train and y_train data sets should be prepared in addition to the training dataset and scaled training data set. By changing x_train and y_train to numpy arrays, you may change the data's two-dimensional structure to three dimensions. Calculate the RMSE after creating the LSTM model and building it. After charting the data and graphically showing them, present the validation and prediction prices. The API Bridge purchase signal should be activated if the validation price is higher than the forecast.

If the valuation price is less than the forecast, turn on the sell signal for the API Bridge. Establish a maximum loss tolerance and the appropriate Stop Loss at the execution of each signal when configuring money management in API Bridge. Establish a profit target before you execute each investment decision utilizing your broker account. Check out the ratios for wins and profits. According to the money management portfolio's instructions, repeat the exercise. One of the most difficult problems in statistics is the financial sector. Many people think that the only method for doing so and enabling them to make some money is technical analysis, but this is not always the case. The Table I and Fig. 3 is representing the analysis and integration of security parameter with various stock values and its entry and exit levels.

For greater effectiveness, several performance metrics can be utilized to combine the various models, such as RMSE, MSE, and MAPE. Annualized ROE, risk-adjusted returns, and volatility have all drawn significant study attention. The mean absolute percent error is used to gauge the accuracy of our forecast system for simulation. Avoiding zeros and extremes will help it work effectively. A complex system execution uses a number of stocks. The trend component dominates the P/E ratio of the company. The famous formula for the Root Mean Square Error is as follows:

$$\mathrm{MAE}=\frac{\sum_{i=1}^{n}|y_i-x_i|}{n} \tag{1}$$

$$\mathrm{MSE}=\frac{1}{n}\sum_{i=1}^{n}\left(Y_i-\widehat{Y_i}\right)^2 \tag{2}$$

$$\mathrm{RMSE}=\sqrt{\sum_{i=1}^{n}\frac{(\hat{y}_i-y_i)^2}{n}} \tag{3}$$

$$\mathrm{MAPE}=\frac{1}{N}\sum_{i=1}^{N}\left|\frac{A_I-F_I}{A_i}\right| \tag{4}$$

Several stock implementations that require high setup hardware resources for concurrent execution may be the main emphasis of the future system [41-43]. It works best when there are no extremes or zeros. The implications and estimation values of ARIMA for Large Cap Enterprises based on Security Parameters are shown in Table II and Fig. 4.

Table II and Fig. 4 show the implications and estimation values of LSTM for Large Cap Enterprises based on Security Parameters.

The vulnerabilities are tuned with SHs and SIs input data, then filtered with SHs and SIs behavioral matrices, the alerts have been generated according to their existing entries of the data. These influenced threshold metrics tuned through ARIMA and LSTM for future analysis of stock values. The authentication mode has synchronized dual and multi authentication modes of execution, which tuned to cross-verify the investors credentials. The experimental scenarios build and experiment to predict the future closing price of Saudi large cap companies and achieved active success rate to analyze vulnerabilities.

TABLE I. IMPLICATIONS AND ESTIMATION VALUES OF ARIMA FOR LARGE CAP ENTERPRISES BASED ON SECURITY PARAMETERS

Security Parameter	Enterprise	MSE	RMSE	MAPE	MAE
{RM, RLCE, DoCP, LWL-T} → {MM, ComM, ConM, SM}	aramco	2.570	0.005	0.001	0.005
{RM, RLCE, LWL-T} → {MM, ComM, ConM, SM}	Sabic	0.000	0.027	0.005	0.025
{RLCE, DoCP} → {MM, ComM, ConM, SM}	Telecom	0.002	0.045	0.008	0.040
{RM, RLCE, DoCP, LWL-T} → {MM, ComM, ConM, SM}	Saudi Electric	0.001	0.0321	0.008	0.027

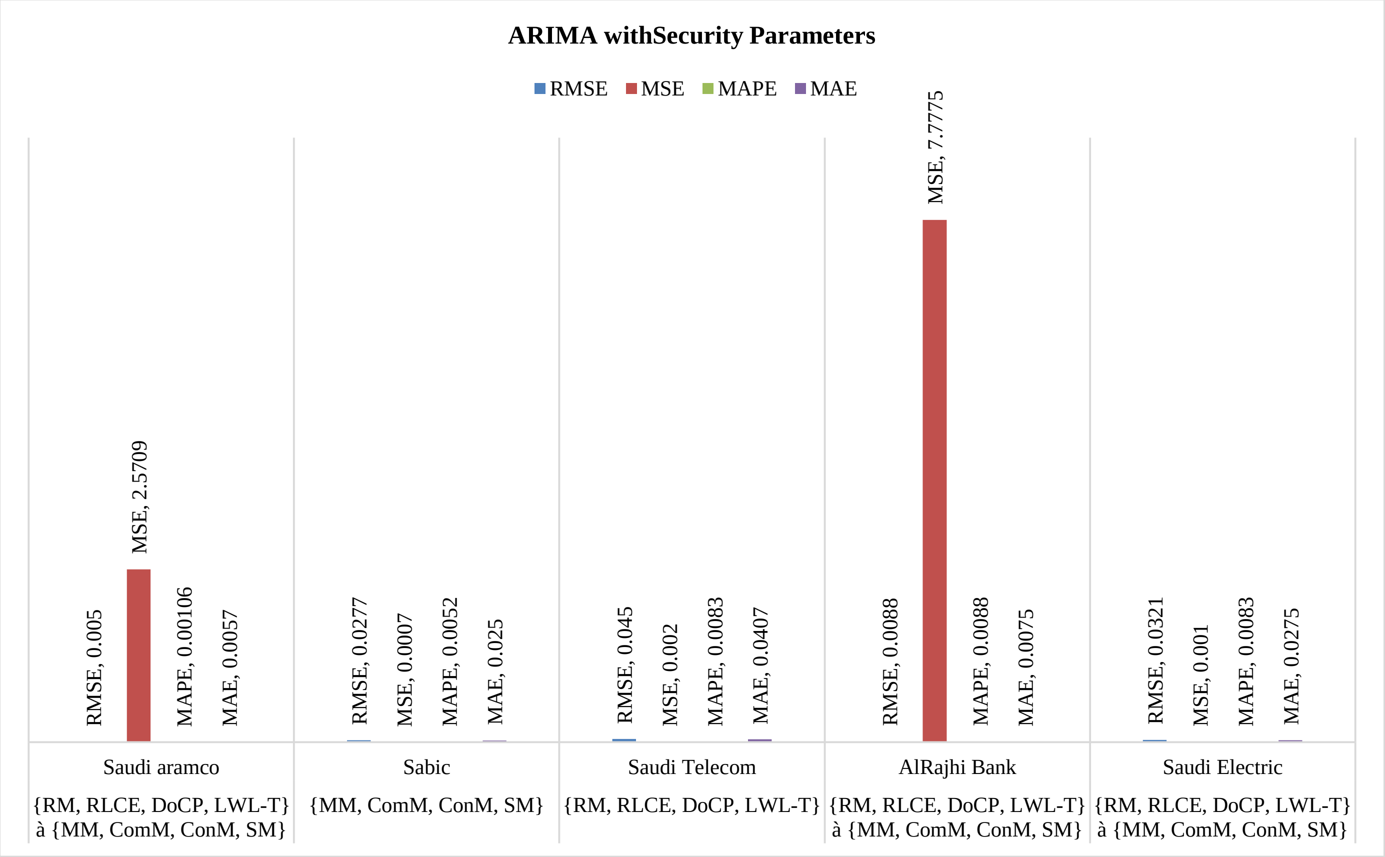

Fig. 3. Implications and estimation values of ARIMA for large cap enterprises based on security parameters.

TABLE II. IMPLICATIONS AND ESTIMATION VALUES OF LSTM FOR LARGE CAP ENTERPRISES BASED ON SECURITY PARAMETERS

Security Parameter	Enterprise	MSE	RMSE	MAPE	MD
{RM, RLCE, DoCP, LWL-T} → {MM, ComM, ConM, SM}	Saudi aramco	0.057	0.238	0.574	0.005
{MM, ComM, ConM, SM}	Sabic	4.860	2.204	1.548	0.015
{RM, RLCE, DoCP, LWL-T}	Saudi Telecom	13.655	3.695	2.487	0.024
{RM, RLCE, DoCP, LWL-T} → {MM, ComM, ConM, SM}	Saudi Electric	1.523	1.234	4.471	0.044

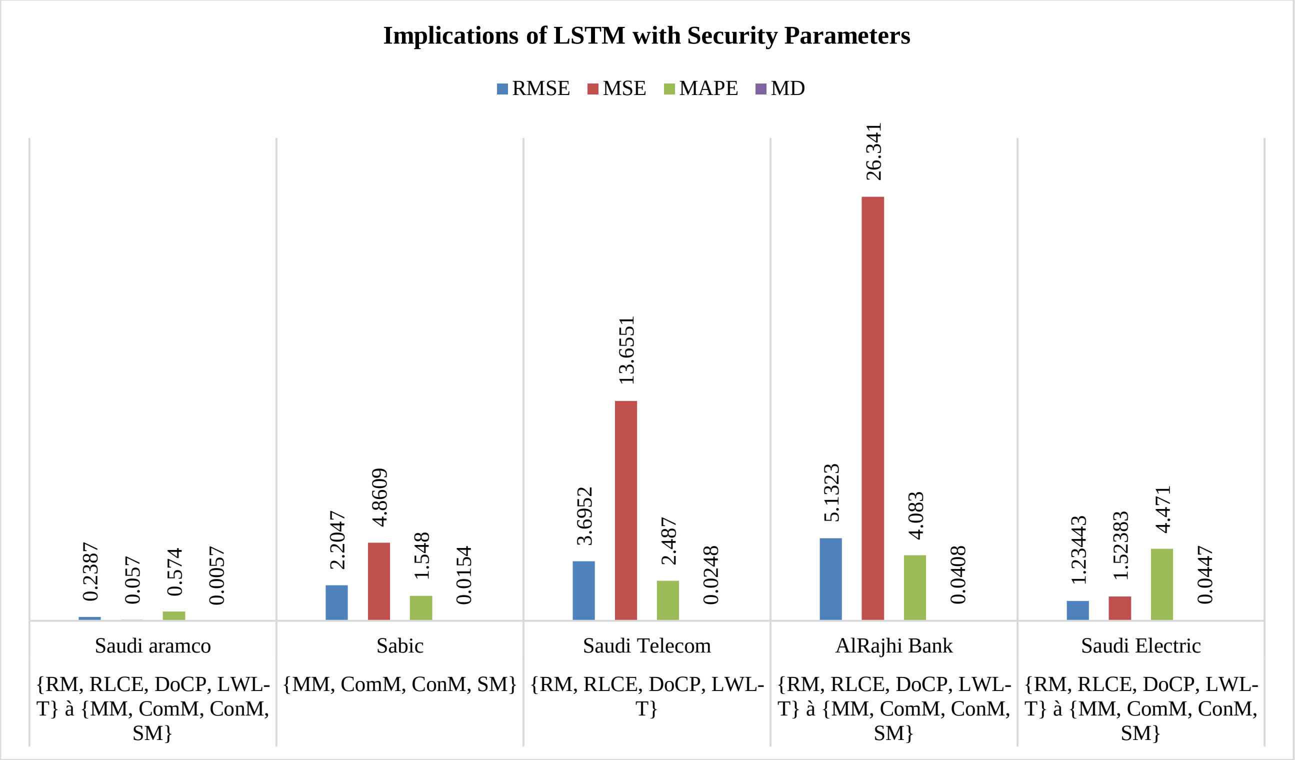

Fig. 4. Implications and estimation values of LSTM for large cap enterprises based on security parameters.

V. Conclusion

This research is proposing layered threshold influenced data security parameters, test cases to control various BOTNETs, DDoS vulnerabilities for stock data validation and integration. It has integrated three layered processes with threshold influenced data security parameters and data metrices to analyze SHs and SIs behavioral entry and exit points. The first layer has framed with RM, RLCE, LWL-T, DoCP environments which tuned with threshold influenced data security parameters which are more influencing stock values. The second layer has framed with MM, ComM, ConM and SM. The third layer framed with expected scenarios and threshold of various vulnerabilities, thread which occurs based on DoS and BOTNETs. All these layers are interconnected together and integrated with behavioral factors of SHs and SIs. The vulnerabilities are tuned with SHs and SIs input data, then filtered with SHs and SIs behavioral matrices, the alerts has been generated according to their existing entries of the data. The authentication mode has synchronized dual and multi authentication mode of execution, which tuned to cross verify the investors credentials. The experimental scenarios build and experiment to predict the future closing price of Saudi large cap companies and achieved active success rate to analyze vulnerabilities.

Funding

This research received no external funding.

Authors' Contribution

Conceptualisation, S.K., Henge; methodology, S.K., Henge., S.K. Mandal., Ravleen Singh; software, Ravleen Singh., S.K., Henge.; validation, S.K. Henge, Madhukar Rane; formal analysis, S.K. Henge, SAS Phani Kumar., Megha Sharma., Gupta; investigation, S.K. Henge., Madhukar Rane., SAS Phani Kumar; resources, Anusha Marouthu, Madhukar Rane.; data curation; writing—S.K. Henge; writing—review and editing, Anusha Marouthu, SK. Henge.; visualisation, Madhukar Rane., Megha Sharma.; supervision, S.K. Henge.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] What is a DDoS Botnet? https://www.indusface.com/learning/what-is-a-ddos-botnet/ (Accessed on 21st July 2024)

[2] What Is A DDoS Attack? https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/ (Accessed on 21st July 2024)

[3] S. Ravikumar and P. Saraf, "Prediction of Stock Prices using Machine Learning (Regression Classification) Algorithms", International Conference for Emerging Technology (INCET), 2020.

[4] A. Sherstinsky, "Fundamentals of recurrent neural network (rnn) and long short-term memory (lstm) network", Physica D: Nonlinear Phenomena, vol. 404, pp. 132306, 2020.

[5] C.C. Emioma and S.O. Edeki, "Stock price prediction using machine learning on least-squares linear regression basis", Journal of Physics: Conference Series, vol. 1734, 2021.

[6] W. Lu, J. Li, Y. Li, A. Sun and J. Wang, "A cnn-lstm-based model to forecast stock prices", omplex., vol. 2020, pp. 6 622 927:1-6 622 927:10, 2020

[7] F. Rundo, F. Trenta, A. L. Di Stallo and S. Battiato, "Machine learning for quantitative finance applications: A survey", Applied Sciences, vol. 9, no. 24, 2019.

[8] Ullah, M. Fayaz and D. Kim, "Improving accuracy of the kalman filter algorithm in dynamic conditions using ann-based learning module", Symmetry, vol. 11, no. 1, 2019.

[9] Ruwei Zhao, "Inferring private information from online news and searches: Correlation and prediction in Chinese stock market", Physica A: Statistical Mechanics and its Applications, vol. 528, no. 15, August 2019.

[10] Shanoli Samui Pal and Samarjit Kar, "Time series forecasting for stock market prediction through data discretization by fuzzistics and rule generation by rough set theory", Mathematics and Computers in Simulation, vol. 162, pp. 18-30, August 2019.

[11] Y. Liu, "Novel volatility forecasting using deep learning-Long Short-Term Memory Recurrent Neural Networks", Expert Systems with Applications, vol. 132, pp. 99-109, 2019.

[12] K. Nam and N. Seong, "Financial news-based stock movement prediction using causality analysis of influence in the Korean stock market", Decision Support Systems, vol. 117, pp. 101-112, 2019.

[13] J. Lee, R. Kim, Y. Koh and J. Kang, "Global Stock Market Prediction Based on Stock Chart Images Using Deep Q-Network", IEEE Access, vol. 7, pp. 167260-167277, 2019.

[14] Chen Mu-Yen, Liao Chien-Hsiang and Hsieh Ren-Pao, "Modeling public mood and emotion: Stock market trend prediction with anticipatory computing approach", Computers in Human Behavior, vol. 101, pp. 402-408, December 2019

[15] Feng Zhou, Zhou Hao-min, Zhihua Yang and Lihua Yang, "EMD2FNN: A strategy combining empirical mode decomposition and factorization machine based neural network for stock market trend prediction", Expert Systems with Applications, vol. 115, pp. 136-151, January 2019.

[16] A, Pathak and N.P. Shetty, "Indian Stock Market Prediction Using Machine Learning and Sentiment Analysis" in Computational Intelligence in Data Mining, Singapore:Springer, pp. 595-03, 2019.

[17] Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese, Insider-threat detection: Lessons from deploying the CITD tool in three multinational organizations, Journal of Information Security and Applications, Volume 67, 2022, 103167, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2022.103167.

[18] F. Kamalov, L. Smail and I. Gurrib, "Stock price forecast with deep learning", International Conference on Decision Aid Sciences and Application (DASA), 2020, pp. 1098-1102.

[19] B. P. Maurya, A. Ray, A. Upadhyay, B. Gour and A. U. Khan, "Recursive Stock Price Prediction with Machine Learning and Web Scrapping for Specified Time Period", Sixteenth International Conference on Wireless and Optical Communication Networks (WOCN), 2019.

[20] G. Li, M. Xiao, Y. Guo, "Application of deep learning in stock market valuation index forecasting", IEEE 10th International Conference on Software Engineering and Service Science (ICSESS) , Oct 2019, pp. 551-554.

[21] Nti IK, Adekoya AF Weyori BA., "A systematic review of fundamental and technical analysis of stock market predictions, "Artificial Intelligence Review,53, 3007–3057. https://doi.org/10.1007/s10462-019-09754-z.

[22] S. A. Alves, W. Caarls and P. M. V. Lima, “Weightless Neural Network for High Frequency Trading”, in International Joint Conference on Neural Networks (IJCNN 2018), pp. 1-7.

[23] Z. Liu, Z. Dang and J. Yu, "Stock Price Prediction Model Based on RBF-SVM Algorithm", International Conference on Computer Engineering and Intelligent Control (ICCEIC), 2020.

[24] J. Cao et al., “Financial time series forecasting model based on CEEMDAN and LSTM” in Physica A: Statistica Mechanics and its Applications, vol. 519, pp. 127-139, 2019.

[25] Zhao, Z., Zhou, H., Li, C., Tang, J.and Zeng, Q.,"Deepemlan: deep embedding learning for attributed networks", Inf. Sci. 543,382-397 ,2021.

[26] Henge, S.K., Rama, B. (2017). Five-Layered Neural Fuzzy Closed-Loop Hybrid Control System with Compound Bayesian Decision-Making Process for Classification Cum Identification of Mixed Connective Conjunct Consonants and Numerals. Advances in Intelligent Systems and Computing, vol 553. pp.619-629, Springer, Singapore. https://doi.org/10.1007/978-981-10-3770-2_58

[27] Henge, S.K., Rama, B. (2018). OCR-Assessment of Proposed Methodology Implications and Invention Outcomes with Graphical Representation Algorithmic Flow. 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_6

[28] S. K. Henge and B. Rama, "Comprative study with analysis of OCR algorithms and invention analysis of character recognition approched methodologies," 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2016, pp. 1-6, doi: 10.1109/ICPEICES.2016.7853643.

[29] S. K. Henge and B. Rama, "Neural fuzzy closed loop hybrid system for classification, identification of mixed connective consonants and symbols with layered methodology," 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2016, pp. 1-6, doi: 10.1109/ICPEICES.2016.7853708.

[30] S. K. Henge and B. Rama, "OCR-Mirror Image Reflection Approach: Document Back Side Character Recognition by Using Neural Fuzzy Hybrid System," 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, India, 2017, pp. 738-743, doi: 10.1109/IACC.2017.0153.

[31] Gupta, R.; Kanungo, P.; Dagdee, N.; Madhu, G.; Sahoo, K.S.; Jhanjhi, N.Z.; Masud, M.; Almalki, N.S.; AlZain, M.A. Secured and Privacy-Preserving Multi-Authority Access Control System for Cloud-Based Healthcare Data Sharing. Sensors 2023, 23, 2617. https://doi.org/10.3390/s23052617

[32] I. Gupta, A. K. Singh, C. -N. Lee and R. Buyya, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions," in IEEE Access, vol. 10, pp. 71247-71277, 2022, doi: 10.1109/ACCESS.2022.3188110

[33] Zhang, D.; Chen, J.; He, Y.; Lan, X.; Chen, X.; Dong, C.; Li, J. A Chunked and Disordered Data Privacy Protection Algorithm: Application to Resource Platform Systems. Appl. Sci. 2023, 13, 6017. https://doi.org/10.3390/app13106017

[34] Yujiao Song, Hao Wang, Xiaochao Wei, Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud", Security and Communication Networks, vol. 2019, Article ID 3249726, 9 pages, 2019. https://doi.org/10.1155/2019/3249726

[35] Ling Sun, Dali Gao, "Security Attitude Prediction Model of Secret-Related Computer Information System Based on Distributed Parallel Computing Programming", Mathematical Problems in Engineering, vol. 2022, Article ID 3141568, 13 pages, 2022. https://doi.org/10.1155/2022/3141568

[36] Lee, J.; Kim, M.; Oh, J.; Park, Y.; Park, K.; Noh, S. A Secure Key Aggregate Searchable Encryption with Multi Delegation in Cloud Data Sharing Service. Appl. Sci. 2021, 11, 8841. https://doi.org/10.3390/app11198841

[37] 52Zhou, Y.; Zheng, S.; Wang, L. Privacy-Preserving and Efficient Public Key Encryption with Keyword Search Based on CP-ABE in Cloud. Cryptography 2020, 4, 28. https://doi.org/10.3390/cryptography4040028

[38] Ehsan Hoseinzade and Saman Haratizadeh, "CNNpred: CNN-based stock market prediction using a diverse set of variables", Expert Systems with Applications, vol. 129, pp. 273-285, 2019.

[39] Rajamanickam, S.; Vollala, S.; Amin, R.; Ramasubramanian, N. Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC. IEEE Syst. J. 2019, PP, 1–12

[40] Thara, E Sampath, P Reddy, "Code Mixed Question Answering Challenge using Deep Learning methods", 5th ICCES, 2020.

[41] Arora, Rajesh, Akshat Agrawal, Ranjana Arora, Ramesh C. Poonia, and Vishu Madaan. Journal of Interdisciplinary Mathematics 24, pp 227-243,2021.

[42] Khurana, Savita, Gaurav Sharma, Neha Miglani, Aman Singh, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Nitin Goyal. Computers, Materials and Continua, pp 629-649,2022.

[43] Gelgi, M.; Guan, Y.; Arunachala, S.; Samba Siva Rao, M.; Dragoni, N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors* 2024, *24*, 3571. https://doi.org/10.3390/s24113571