International Journal of Innovative Research in Engineering
Volume 3, Issue 3 (May-June 2022), PP: 74-77.
www.theijire.com
ISSN No: 2582-8746

ATM Fraud Identification Using Machine Learning

Jim Mathew Philip[1], E. Parvish Musaraf[2], S.Shyamala[3], Surya Kumar[4]
[1] Assistant Professor (Selection Grade), Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore-641 010, Tamil Nadu, India.
[2,3,4] Final year B.E(CSE), Sri Ramakrishna Institute of Technology, Coimbatore-641 010, Tamil Nadu, India.

How to cite this paper:
Jim Mathew Philip[1], E. Parvish Musaraf[2], S.Shyamala[3], Surya Kumar[4], "ATM Fraud Identification Using Machine Learning", IJIRE-V3I03-74-77.

Abstract: *In today's environment, computer networks are vital for making communication processes more efficient and agile. The increasing requirement for data transmission volume and agility, as well as the ongoing convergence of these operations to the Internet, mandates the employment of larger and more dependable computer networks. As a result, establishing new ways and tools to assist with this management is vital to assuring the quality of services provided. These tools must be efficient and have a low computing cost in order to allow the research of large scale networks. Furthermore, the process of face recognition and identifying problems should be carried out without the involvement of humans, a topic of research known as Autonomic Management. Withdrawal from an ATM (Automated Teller Machine) system using LINK technology and a card reading device two step of authentications for security face recognitions and otp checking. Withdrawal from an ATM (Automated Teller Machine) system using LINK technology and a card reading device. An attacker can simply conduct fraudulent withdrawals if he obtains an ATM card and pin number. As a result, we recommend a system that incorporates an ATM card scanning system as well as a LINK system. By scanning his card, this individual can gain access to the system. However, once the user has finished the authentication process, he can view the data, but if he chooses the money withdrawal option, he will be requested to enter the LINK machine learning for linear regressions algorithm. This strategy decreases analysis complexity while enhancing network stability and accessibility, allowing administrators to swiftly spot defects, threats, and system failures. As a result, this study employs a variety of traffic characterization models, including the Digital Signature of Network Segment utilizing Flow Analysis (DSNSF), the (ARIMA) approach, and Principal Component Analysis (PCA). Proposed Map Reduce Based Holt Winters Method and Principal Component Analysis (PCA). The DSNSFs derived by the proposed models are compared to real-world traffic of bits and packets in a real network environment, and then submitted to particular tests to determine their accuracy. The suggested approach produces a workable solution that is a significant advance over current systems.*

Keywords: *Computer networks web ATM, Network management system, Prediction method, Forecasting method, security, face recognitions otp security*

I. INTRODUCTION

Computer networks are as important as piped water, electricity, and telephone service in today's civilization. Its operation cannot be disrupted due to the importance of its services to the individuals who utilize them. In this setting, network management automation becomes critical for lowering costs, minimizing performance bottlenecks, and detecting network faults early. Determining regular network activity is a crucial step in detecting traffic abnormalities. For traffic characterization, we employ the DSNS (Digital Signature of Network Segment) created by the BLGBA (Baseline for Automatic Backbone Management) model. The DSNS is a collection of fundamental data that Persuasive Cued Click-Points (PCCP) is an integrated evaluation of the graphical password system, encompassing usability and security. The systematic review provides a full and integrated assessment of PCCP, including both usability and security concerns. One of the most significant usability goals for knowledge-based authentication systems is to assist users in picking higher-security passwords from a larger effective security space. This research project looks at the feasibility of developing and building a module that can be simply integrated into existing authentication systems. The working prototype is an open source simulation that includes all of the components required to construct the authentication system. Although numerous database systems may be used, this system is designed with Java and Oracle 10g Express Edition as the database. It displays the traffic profile on a server or network segment, At every given time, it is important to acquire a close-to-real prediction of the traffic characteristics of the segments that make up the network backbone. In addition, traffic classification is critical for network security management. The usage of the
DSNS can provide more detailed information on traffic patterns. The expected knowledge of a segment's or server's traffic characteristics is closely tied to the profile of its usage, and this information may be utilized to spot abnormalities, minimizing

network downtime and enhancing network dependability.

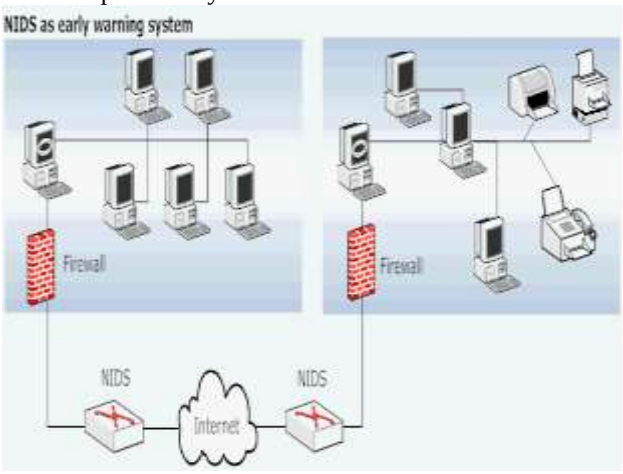

Fig 1: Network Management System

II. RELATED WORK

R. Fontugne, et.al,… [4] supplied a time interval strategy that may be adjusted to improve the detection method's robustness in the face of traffic changes This adaptive anomaly detection system is compared to three other anomaly detectors using four years of real backbone traffic. The advantages of this adaptive method are demonstrated by comparing the findings of this adaptive method to those produced using fixed parameter tunings and those of three other anomaly detectors using four years of actual Internet data. In terms of true detection, the proposed adaptive detection methodology outperforms the previous methods. supplied a time interval strategy that may be adjusted to improve the detection method's robustness in the face of traffic changes This adaptive anomaly detection system is compared to three other anomaly detectors using four years of real backbone traffic.positive and false positive rates, according to the assessment.

Wang, We, et.al, [1] proposed a new intrusion detection method based on Principle Component Analysis. Instead of considering the transition information of the system calls or commands, the new method takes into account those of frequency property. Since there is no need to consider each system call in each trace or command in each block, the computational cost of the proposed method is low and suitable for real-time intrusion detection.

X Song, et,al,… [2] used a scientific method in which the various data qualities are divided into environmental and indicator attributes, and a new observation is regarded anomalous if its indicator attributes cannot be explained in the context of the environmental attributes. While the model may always be used to check for new abnormalities fast and effectively, training the model on a multi-gigabyte database may be slow without modifying the techniques.Huang, et,al,…

[3] introduced a novel algorithmic framework for detecting network
anomalies that combines distributed tracking with PCA analysis to find abnormalities with far less data than earlier approaches. Local filters, placed at each monitoring site, are used to choose parameters based on global criteria in the distributed tracking system. The objective is to track only enough local monitoring data to allow accurate detection. Local filtering decreases the quantity of data sent over the network, but it also implies that anomaly detection is confined to partial or limited views of the global state.

Lazarevic, Aleksandar, et.al,… [5] For identifying new assaults whose nature is unknown, various anomaly and outlier detection algorithms have been presented. A mechanism for extracting additional valuable characteristics is also created to aid the anomaly detection framework. Furthermore, the assessment of anomaly detection methods is carried out using both standard and customised metrics that are particularly useful in identifying intrusions involving many network connections. In today's Web-enabled world, reliable user authentication is becoming increasingly crucial. In a business or enterprise context, the repercussions of an unsecured authentication system may be disastrous, including the loss of private information, denial of service, and data integrity compromise. The importance of secure user authentication extends beyond computer and network access. There are several additional applications in everyday life. Everyday life also require user authentication, such as banking, ecommerce, and physical access control to computer resources, and could benefit from enhanced security.

III.EXISTING METHODOLOGIES

Anomalies in network traffic are odd and substantial variations in a network's traffic. In today's social and economic infrastructures, networks are critical. The network's security becomes more critical, and network traffic anomaly detection is a key aspect of network security.

3.1 Key security model:

ATM machines can be used to deliver banking services in low income countries where only a few people use banks. Interactive Automated Teller Machines, that can dispense and take deposits, help increase financial literacy and facilitate the access to formal financial services in remote areas. Two thirds of the world’s population depend on hard cash. Most of these people reside

in developing countries where a large portion of them is unbanked. Therefore, the importance of ATM machines in financial inclusion cannot be underestimated. So offering financial inclusion is an advantage of ATM machines.

$$Z_t - \sum_{i=1}^{p} \emptyset_i Z_{t-i} = e_t - \sum_{j=1}^{q} \theta_j Z_{t-j}$$

Where $e_t$the forecast error at time t, ϕ and θ is are the auto regressive and moving average coefficients of finite order p, q, respectively. Yet, the original time series is differentiated d times in order to obtain at, the integrated part of the model. The creation of Digital Signature of Network Segment using Flow analysis (DSNSF) from the ARIMA model occurs dynamically using the past weeks data for training and the changes in every new day processed to recalibrate the model.

3.2 Principle component analysis:

The proposed system aims to solve all this by constant updating of bank records. The Web based construction of the system will enable transactions at any bank or ATM to be registered within a matter of seconds. Security of these details is also a top priority in this system. This central hub will be accessed by an ATM for secure customer transactions. In our project we are going to place an extra button in ATM machines. When that button got pressed the control window will be telecasted to accountant cellular phone. Then the accountant can enter the pin and amount manually in his mobiles telecasted pop-up window. By this control system accountant can keep his pin number with him and he can vend the amount by his own control by the desired person

y= Dependent Variable.

x= Independent Variable.

a0= intercept of the line.

a1 = Linear regression coefficient.

is diagonalized, i.e., the variance along the principal components φ1,...,φK is maximized and the off-diagonal components are minimized.

IV.PROPOSED METHODOLOGY

The existing methodologies can't detect big data based network data streams and redundant data can be appears in prediction stage. These limitations are overcome by proposed approaches such as map reduce based Holt winters method.

Automatic Teller Machine (ATM) in future will have mobile security authentication techniques to verify identities of customer during transaction.

4.1 Machine learning algorithm:

Machine learning liner regressions algorithm , Records it is dealt with isolation by tasks called the Machine learning The output of the Mappers is then got together within into the second set of tasks names the Reducers, where outputs form various Mappers can be joined together. Problem fitting for treating with Machine learning have to usually be readily separated into independent subtasks that can be treated in parallel. The master node gets the input and splitting into smaller sub problems then dispenses then to worker nodes that may do this again in turn which leads to a multi level structure of tree. The worker node treats the passes answer block to its master node and smaller problem reduce step. The master node collects the solutions to all of the subproblems and puts them together in some fashion to find a solution to the problem. We can use this framework to input network data streams and remove superfluous data using a multi-level structure.

4.2 Web Processing method:

A user is a person who uses a computer or network service. Users generally use a system or a software product without the technical expertise required to fully understand it. In the user module have some sub modules such as,

- Accessing ID
- Check the ATM Card Number
- Face Recognitions
- OTP generations
- Visually Generated Report

In this paper we use an improvement of the traditional Holt-Winters method called Holt Winters for face Digital Signature (HWDS), which modifies the equations that describes the baseline and linear trend in order to achieve better results on the traffic characterization. There are two versions of this approach, each with a different seasonal component. When seasonal variations are

fairly constant across the series, the additive technique is recommended, while the multiplicative method is preferable when seasonal variations change proportionally to the series level. The seasonal component is expressed in absolute terms in the scale of the observed series using the additive approach, and the series is seasonally adjusted in the level equation by removing the seasonal component. The seasonal component will equal zero at the end of each year. The seasonal component is expressed in relative terms (percentages) using the multiplicative approach, and the series is Seasonally adjusted by dividing through by the seasonal component. Within each calendar year,

$$\hat{y}_{t+h|t} = (l_t + hb_t)s_{t-m+h_m^+}$$

$$l_t = \alpha\frac{y_t}{s_{t-m}} + (1-\alpha)(l_{t-1} + b_{t-1})$$

$$b_t = \beta^*(l_t - l_{t-1}) + (1-\beta^*)\, b_{t-1}$$

$$s_t = \gamma\frac{y_t}{(l_{t-1} + b_{t-1})} + (1-\gamma)s_{t-m}$$

And the error correction representation is:

$$l_t = l_{t-1} + b_{t-1} + \alpha\frac{e_t}{s_{t-m}}$$

$$b_t = b_{t-1} + \alpha\beta^*\frac{e_t}{s_{t-m}}$$

$$s_t = s_t + \gamma\frac{e_t}{(l_{t-1} + b_{t-1})}$$

Where $e_t = y_t - (l_{t-1} + b_{t-1})s_{t-m}$

As a specific case of the Holt-Winters method without seasons, Holt two-parameter linear exponential smoothing is offered. To account for typical seasonal swings in a series, the winter's approach (also known as Holt-Winters) combines a temporal trend with multiplicative seasonal variables.

V. CONCLUSION

Facial verification software is used in an ATM model to ensure security. When facial recognition technology are combined with the identity confirmation process used in ATMs, forced transactions can be greatly reduced while still providing hard-secure authentication. Because facial recognition appears to be more difficult than other biometrics, a more efficient algorithm can be devised. When beard and ageing can be corrected, erased, or decreased, the inability to detect the face. If the expense of face recognition is too high, retinal or iris recognition can be utilized instead. We plan to add an additional button to ATM machines as part of our initiative. The control window will be transmitted to the accountant's cell phone when that button is hit. The accountant can then manually input the pin and amount in the telecasted pop-up window on his mobile phone. This control mechanism allows the accountant to have his pin number on hand and to vend the money under his own supervision to the chosen individual.

References

[1] R. Babaei, O. Molalapata and A. A. Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rd ed. vol.45, pp.211-216, 2012.

[2] Aru, O. Eze and I. Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online] 2013, pp. 188-193.

[3] K. J. Peter, G. Nagarajan, G. G. S. Glory, V. V. S. Devi, S. Arguman and K. S. Kannan, Improving ATM Security via Face Recognition, in ICECT, Kanyakumari, 2011, vol.6, pp.373-376.