Journal of Android and IOS Applications and Testing
Volume 3 Issue 2

A Novel Defence Mechanism Against Man-In-The-Browser Attacks Using Ais

Bejoy B J, Dr.S. Janakiraman, Ilankadhir.M
Department of Banking Technology
Pondicherry University

Abstract

Man-in-the-Browser (MitB) attacks are a category of Man-in-the-Middle attacks that is considered as the topmost menace to online banking by many professionals. In MitB, a proxy trojan implants itself into the browser of the user and alters thetransactions done by the user. This trojan is imperceptible to the user and also it changes its signature making it difficult to bespotted by antivirus program. Here attackensues before encryption and after decryption in thebrowser. In this paper, an Artificial immune system (AIS) based model is proposed which uses Natural Killer Cells (NK) to alleviate the attack of MitB trojan. Here user profile is created centered on the user's history of transactions. Two types of NK cells are created-negative selection based NK cells (NSNK) and positive selection based NK cells (PSNK). The incoming transaction details are converted to Major Histocompatibility complex (MHC1) molecules. Then it is supplied to NK cells. If it is detected by NSNK, then it may be an unauthorized transaction and three-factor authentication is applied. If MHC1 is detected by PSNK, then it is considered as authentic and the transaction is free to occur using the default two-factor authentication mechanism.

Keywords: *MitB, AIS, NSNK Cells,PSNK cells, MHC1,three-factor authentication*

INTRODUCTION

Internet finds many applications nowadays. One of the important application of internet it the banking sector is the usage of internet for online banking. Due to the comfort of online banking, many users are fascinatedby online banking. According to Financial Express, there are an active 45 million urban banking users in India currently and is on the rise immensely. As online banking grows, so is the misuse of it. There are around 26,000 online banking fraud cases reported and ≠179 crore lost in 2017 in India as reported by [1]. Eventhough many security measures are used to minimize banking fraud; it is still on an escalation. Attacks such as phishing, pharming, and Man-in-the-Browser(MitB) attacks have bested the demand list of online attackers. An overview about MitB is given and how MitB is used for online banking attacks are elucidated in this part.

Man-in-the-Browser attacks

The term Man-in-the-Browser was first used in [2]. In MitB, first a dropper is installed in the user's computer which downloads all the other modules and thus a proxy trojan implants itself into the browser hooking the security functions of the browser. When a user tries to access some predefined websites like online banking sites, the Trojan is elicited. The trojan then intercepts and alters the data that is exchanged between the client browser and the bank server without the knowledge of the banking user. Some features of the banking trojans include ascreenshot, video capture, keystroke logging, cross-site scripting and setting up a remote server. Even the TLS/SSL encryption mechanism cannot escape the MitB trojans. Because the browser's certificate checking and security functions are also hooked. The modification of user data in a transaction happens before the

data is encrypted when it is sent and after decryption when it is received. The signature of the banking trojans keeps on changing making it difficult for antivirus programs to catch it. This makes MitB more treacherous to online banking users. Zeus [3] is the most widespread and low detected trojan of all the MitB's that was first detected in 2007 followed by its predecessor Game overZeus(GOZ) [4] both designed by Evgeniy Bogachev which is mainly used as a banking trojan. The other serious threat to online banking was SpyEye [5] designed by Aleksandr Andreevich Panin and Hamza Bendelladj which was detected in 2009.Other examples include Silent banker [6], Tinybanker [7] and Hesperbot [8].

There has been an exponential growth in the features of MitB used for online banking attacks. A survey on behaviors of various MitB trojans is described in [9]. MitB is continuously evolved while protections against them are still based on old methods. MitB even has a mobile phone version called as Man-in-the-Mobile attacks(MitMo) which affect Android, Symbian and IOS phones. Thus traditional security mechanisms like antivirus software, two-factor authentication, TSL/SSL certificate, mobile OTP, smartcard etc. will not help in evading MitB attacks. Existing defend mechanisms [10] are not effective in extenuating MitB. These include Out-of-Band authentication (OoB), ahardened browser with no plug-ins installed used only for net banking, transaction methods etc. Mechanisms like OoB are compromised due to theavailability of MitMo. Trojans are fully automated to perform all the functions without manual help from installation to changing the transaction details (Fig 1). In this paper, an AIS based mechanism that alleviates the impact of MitB in online banking application is described that uses natural killer cells of theinnate immune system. This system is implemented on banks server-side making it comfortable for the user in online banking.

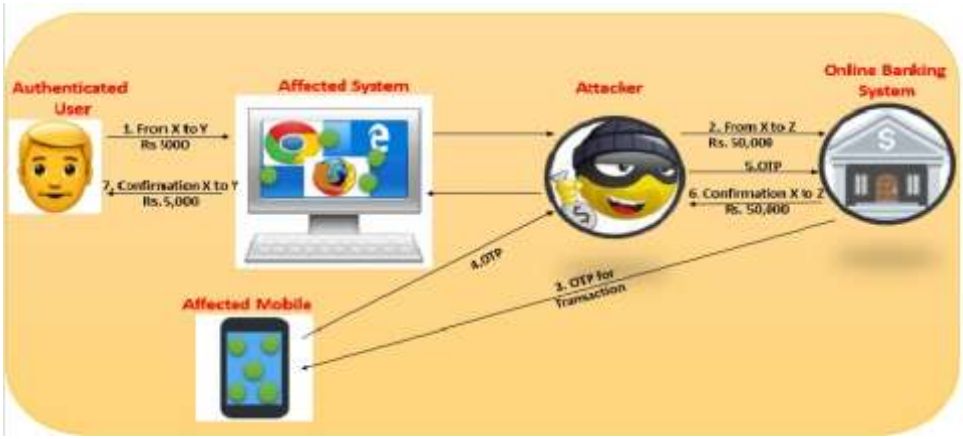

Fig 1. *Functioning of MitB in Online Banking*

RELATED WORK

Because of the privacy of banking and unavailability of online banking data due to secrecy, alimited numbers of works were available for reference. So works in online banking fraud detection, credit card fraud detection and other fraud detection methods along with intrusion detection system(IDS) can be used for this approach. IDS and credit card fraud detection have aresemblanceto online banking fraud detection. This motivated us to review such works also for designing a novel framework for defending against MitB attacks in online banking. A model was developed [11] that used differential

analysis for online banking fraud detection by generating global and local behaviors of the users. Global analysis and differential analysis was used in this approach. Device fingerprinting was used to identify the device used for banking. Black, white and suspect list was used in theglobal analysis. A transaction using blacklisted devices was considered fraudulent whereas transaction using whitelistwere considered authentic. Devices which were not in either list were added to suspect list.Differential analysis was used to determine the deviation of current transaction from theaverage transaction of the user based on payment transaction frequency, attempted login failures and frequency of logins. The risk was calculated based on global and local analysis by using Dempster-Shafer theory.

Another fraud analysis mechanism was used which used Trend Offset Analysis(TOA) [12] for detecting fraud. TOA uses three steps namely Signature assessment, deviation of signature from current behavior and fraud detection to get results.TOA uses a sliding window for calculating the signature of the user adding current transaction and discarding old transaction. The current transaction is compared with this signature and deviation from the signature is calculated. The Classification and Regression Tree (CART) is used to analyze the fraud. A fuzzy theory-based model [13] was proposed for identifying user behavior uncertainty. Here customer behavior was classified into normal and suspicious behavior. A fuzzy rule base was created based on input parameters and views of banking experts. Around 120 if-then rules were developed to detect fraud using the fuzzy expert system. At last,a ROC (receiver operating characteristic) curve was used to examine the fuzzy expert system.

An ontology-based system for detecting fraud [14] is used. An activity database is created based on user activities by the server. The database stores all the activities of an account in ontology instance. These ontologies help to find frauds based on some rules formed by the activity. Ontologies are inserted and deleted based on the utility of ontology for fraud detection. Some parameters used for ontology creation are time data, geographical data, navigation habit data and webpage data. A threshold is used to differentiate the new behavior from old behavior. The use of local, global and temporal profiling [15] was used for fraud detection in online banking and credit card transactions. Is was a decision support system that was used for fraud and anomaly detection.Histogram-based outlier score(HBOS) method was used to calculate the local profile by using min-max normalization and assigning weights to each parameter. Classes of user spending were used to create a global profile and DBSCAN algorithm was used to cluster the global profile and a score was calculated based on the distance between the profile and its nearest cluster. In temporal profile, mean and variance of the transaction were calculated and were used as athreshold for calculating anomaly score.

Some methods use theartificial immune system for fraud detection. Artificial Immune Recognition System (AIRS) [16] was used to analyze the user behavior as well as fraud. Based on the previous transactions a normal detector is created for a user. Fraud detectors are also created based on some transactions that are fraud. To detect fraud of a user, thenormal detector of the user, as well as k neighbors from fraud detectors, is chosen to determine fraud. This model was enhanced using an Artificial Recognition Ball (ARB) [17] which reduces duplicates. This method uses cloud computing techniques. Hadoop and MapReduce were used for

parallel processing. Negative selection along with clonal selection was used to achieve more precision in fraud detection. A risk rating is given to each transaction for identifying the fraudulent transaction.
Many works in IDS also forms the basis of fraud detection because of the similarity in their nature to detect anomalies. A multi-agent based system was used [18] which worked in virtual machines for detecting anomalies. Detectors were created randomly and thenegative section was used to eliminate self-recognizing detectors.The detectors which detect alarge number of attacks were cloned and these mobile agents were migrated to virtual machines. Immune network algorithm was used for communication between cloned agents. A detector moving algorithm [19] was proposed that allow the overlapped detectors to adjust the radius to minimize the overlapping. Random detector generation along with negative selection was used for creating new detectors. This approach was used to detect faults in a DC motor. A detailed survey of AIS based IDS was given in [20]

The survey helps us to conclude that a user profile based fraud detection system is efficient which can be used to mitigate the effects of MitB in an online banking system. The detection of fraudulent transactions should be in real time. The behavior of customer as well as banking trojans is dynamic. A fully efficient system for mitigating MitB still lacks due to various reasons.

PROPOSED WORK

An AIS based system that uses Natural Killer(NK) cells is designed to ease the attack of MitB trojans on anonline banking application. AIS concepts like Negative selection, Positive selection and Clonal selection are used in this paper to generate cells that have the capability to identify fraudulent transactions initiated by MitB trojans. Negative selection to create fraud detection cells, Positive selection to create normal cells that identify normal transaction and clonal selection algorithm to proliferate high fitness value cells.

Natural Killer (NK) Cells

Natural killer cells are a type of innate immune lymphocytes that kill infected cells in Human Immune System (HIS). They were thought to be the main backbone of innate immunity; recent research proves that they have immunological memory also. They have aquick response to cancer or tumor affected cells as they only look for the presence of MHC1 in target cells. If MHC1 is down-regulated, they perform apoptosis (programmable cell death) of target cells. Hence the name natural killers. They have two types of receptors- an Activation receptor and an Inhibitory receptor which decides what action to be performed on the target cell i.e. either to kill the cell or identify the cell as normal. A Natural Killer Cell is shown in Fig 1.

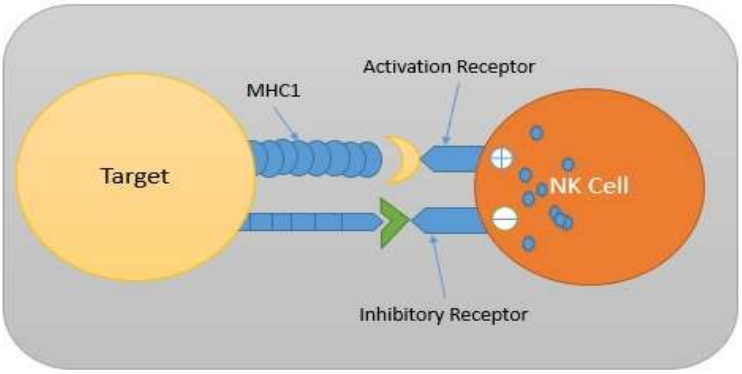

Fig 2. *NK Cells*

Artificial NK Cell

An artificial NK cell is defined as an independent cell that has the capacity to interact with other cells and can find a fraudulent transaction in an online banking system. An artificial NK cell is defined by

NK (Type, Radius, Fitness, State)

Type: Type defines the type of NK cell whetherNegative Selection based NK cells (NSNK) and Positive Selection based NK cells (PSNK).

Radius: It defines the range of the NK cell. If the incoming data is within the radius, NK cell is activated.

Fitness: IT defines the fitness value of NK cell. When it detects more data, fitness value increases.

State: A NK cell can be in any of the sixstates. The states are described in table 1.

Table 1. *States of an NK Cell*

States	Description
Inactive	Initially in theInactive state
Active	When it encounters MHC1
AR	When MHC1is inside NKR
IR	When MHC1 is outside NKR
Mature	When Health value reaches Threshold
Emulate	NK is emulated until a MaxPop is reached

Initially, NK cell is in inactive state. When it receives an MHC1, it is transferred to anactive state. In theactive state, it checks MHC1is inside NK radius or not. If MHC1 is in NK radius is in (NKin), NK changes to Activating Response (AR) state. If it not outside Nk radius (NKout), the transaction is considered normal and NK state is changed to Inactive. In AR State, it checks whether fitness is greater or equal to fitness threshold (FT), the NK cell state is changed to mature state. In thematurestate, if no of NK cells is less than maximum population (MaxPop), then the NK cell is proliferated and then it goes into theinitial state. While in amature state, if anumber of NK cells is equal to MaxPop, then the NK cell state changes to inactive state. State transition diagram of an artificial NK cell is given in Fig 3.

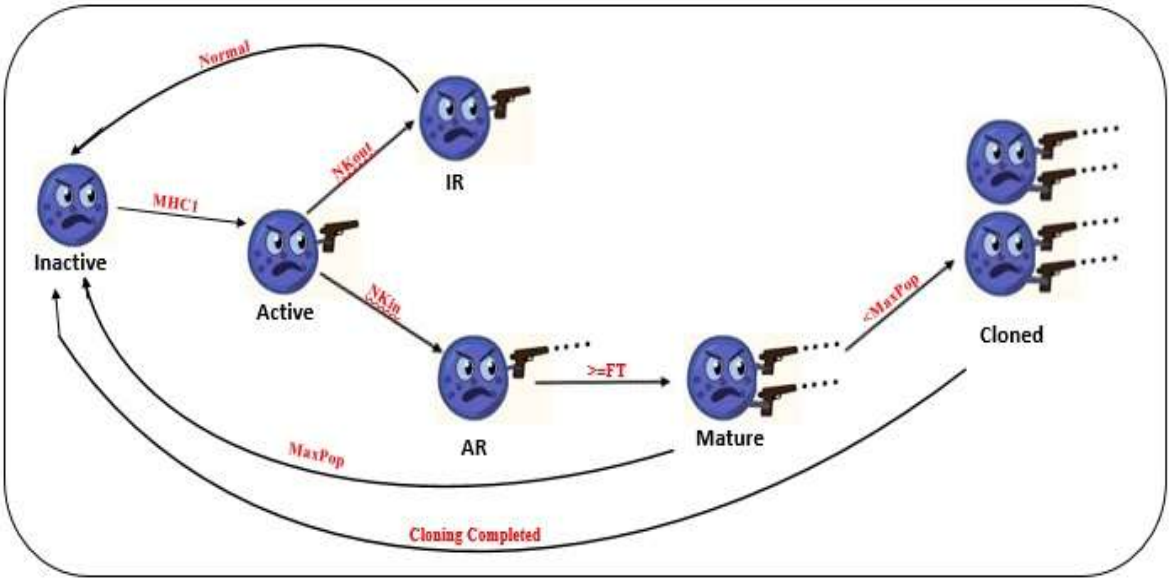

Fig 3. *State Transition Diagram*

NK Cell-based System

The proposed system maintains two databases for keeping track of blacklisted IP's(BLIP) as well as blacklistedlocations(BLL). BLIP contains the list of well-known IP addresses that are used by attackers and BLL contains the list of known places whose banks are used for cyber-attacks on online banking. The system has two types of NK cells NSNK and PSNK.NSNK cells are based on Negative selection algorithm and PSNK are based on Positive selection algorithm. PSNK contains NK cells that detect normal behavior while NSNK contains cells that detect fraudulent transaction.NSNK cells are generated and their radius is set based on Eq.1.

$$NKR = Min\{ \forall |d - r_i| \text{ where } i=1 \text{ to } n \} \quad (1)$$

Where d represents the distance between the center of the cell randomly generated to the self-points in the system and r represents the radius of the self-points. Thus, the radius of NK cell is thus based on the nearest self-point. PSNK cells are created based on the self-radius r. The incoming packet is converted to MHC1 using Eq.2.

$$MHC1 = \sum_{i=1}^{n} P_i * W_i \quad (2)$$

Where *P* stands for the parameters considered and *W* stand for the weightage given to each parameter to detect banking fraud. The parameters used in this approach are given in table 2.

Table 2. *Parameters Used*

Parameter	**Description**
Source IP	The IP address of user's system
Browser fingerprinting	Browser used by the user
Operating System	The operating system used by the user
Destination bank	The destination bank
Destination location	The location of destination bank
Credit account	Account of the receiver
Amount	The amount of each transaction
Balance	Balance after Transaction
Timestamp	Timestamp of the transaction

The architecture of NK cell-based fraud detection system is given in Fig 5.BLA is the Blacklistanalyzer that checks the IP address and destination branch location is on theblacklist. If the IP address is on theblacklist, the transaction is marked as fraudulent. If location is in BLL, then thetransaction is marked as Suspicious. If both lists are no match BLA converts the incoming transaction into MHC1 and supplies it the PSNK cells. If PSNK cells detect transaction then, the transaction is marked as authentic and the no more processing is done. If MHC1 is not detected by any PSNK's then the MHC! Is given to Promiscuous Analyser, that takes a copy of the MHC1 and gives it to various analyzers for parallel processing of MHC1.The analyzers perform load balancing by giving the transaction to various NSNK cells. If any NSNK detects as MHC1(Fig 4), then the transaction is marked suspicious and a third-factor authentication mechanism is activated. This third factor may be a biometric authentication or a voice-based authentication [21]. If a fraudulent transaction is authorized by the author two times using third-factor authentication, a PSNK cell is created based on the MHC1 for that transaction and the NSNK detector that detects it is deleted from the population.

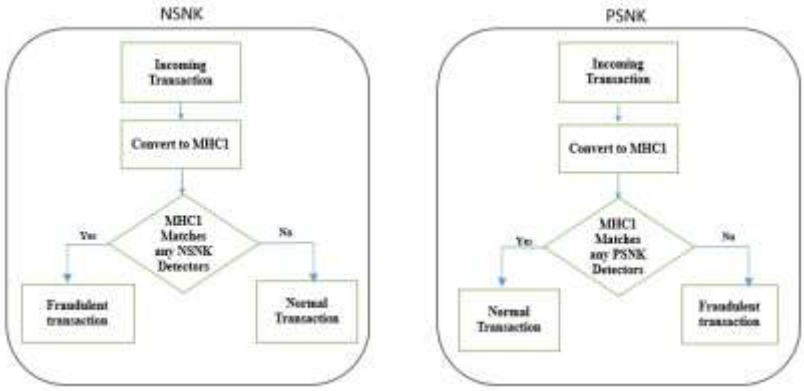

Fig 4. *Working of NSNK and PSNK cells*

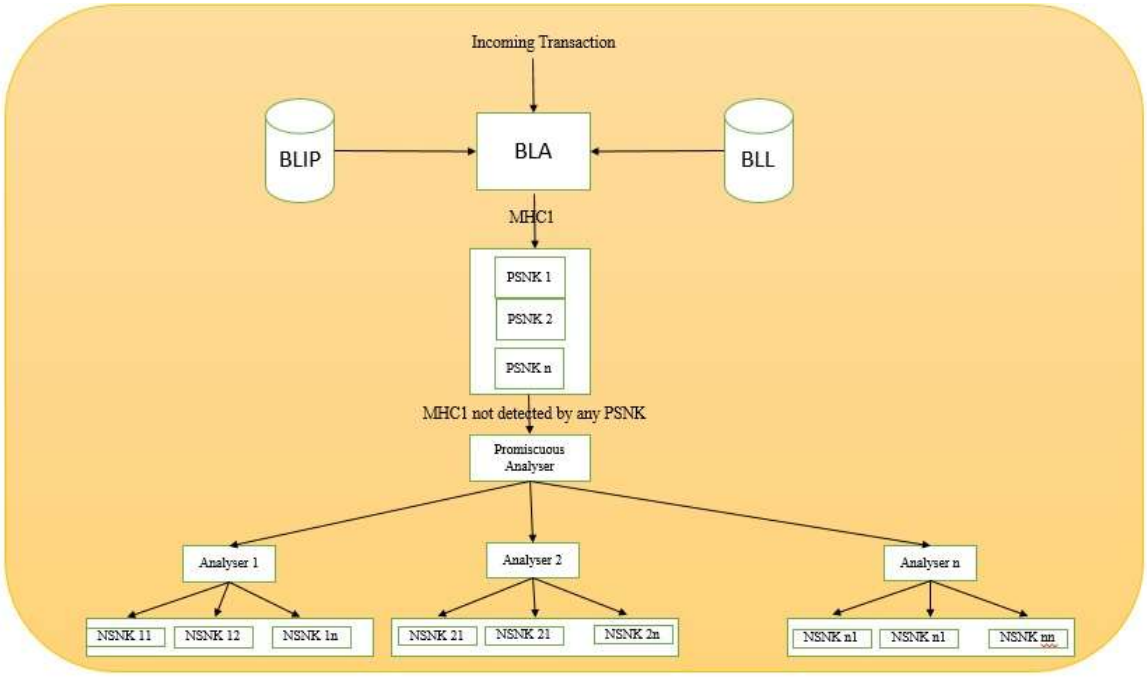

Fig 5. *The architecture of NK cells*

RESULTS AND DISCUSSION

Due to the secrecy of banking domain, online banking datasets was not easily available. So we are enhancing the trans.asc file of Berka dataset [22] for evaluating our approach by adding fields like source IP, Browser fingerprinting, user OS, labels etc. We are not concentrating too much on the dataset as our main aim was to design an efficient system against MitB attacks.Dataset was preprocessed and min-max normalization was applied to make it between 0 and 1. We took two types of data from the dataset for evaluation.

We compare our work with that of Kancherla [12] and Soltani [16]. We use two parameters Detection rate and false positive rate to evaluate our approach.

Detection rate is calculated as the ratio of normal transaction identified as normal to the total number of normal transactions in the dataset expressed in Eq 3.

Detection rate=True positive/ (True positive +False negative) *100 (3)

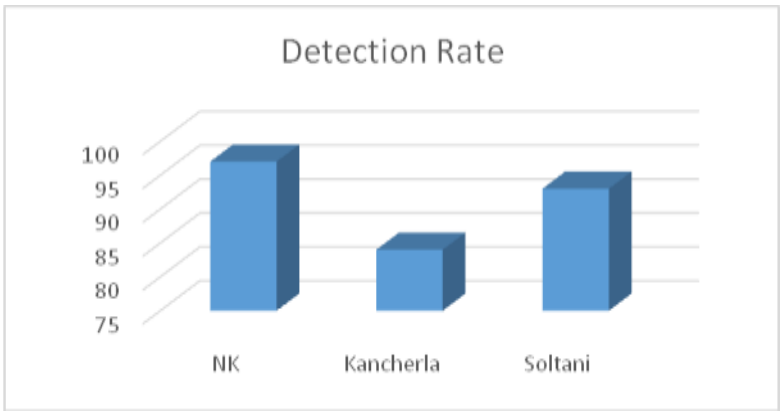

Fig 6. *Detection Rate*

Our approach shows a detection rate of 97 % compared to Kancherla and Soltani with 84% and 93% respectively (Fig 6). The false positive rate is defined as the ratio of atotal number of abnormal transactions identified as normal to the total number of abnormal transactions in the dataset expressed by Eq.4.

False Positive Rate=False Positive/ (False Positive +True Negative) *100 (4)

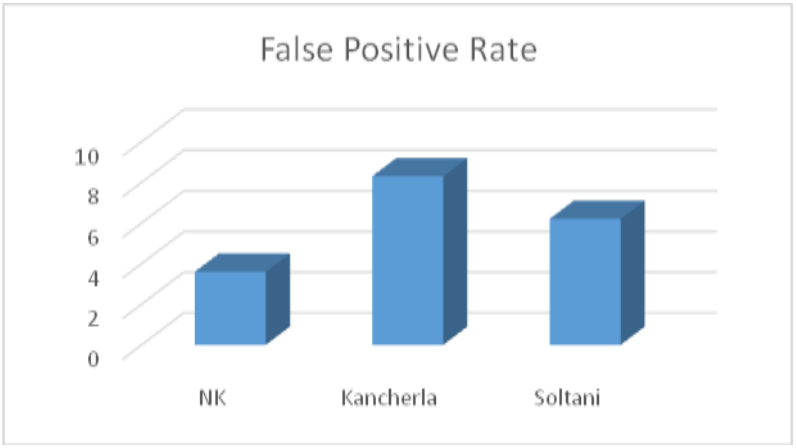

Fig 7. *False Alarm Rate*

The approach using NK cell shows low false positive rates when compared to other two approaches Fig 7. The result may vary in real time because the dataset used may not be too stable as it is the extended version of theoriginal dataset.

CONCLUSION AND FUTURE WORK

A Natural Killer cell inspired AIS model for alleviating the attack of MitB trojan on internet banking is proposed in this work. NSNK cells were created using negative selection to identify fraudulent transaction and PSNK cells were created using positive selection algorithm to detect normal behavior of the user. High fitness NSNK cells were proliferated using clonal selection algorithm. Implementation results show that this approach is far better than the works compared in the literature. This work can be used for other fraud detection mechanisms like credit card fraud detection and even for intrusion detection system by adjusting the parameters used to evaluate MHC1.The extended version of Berka dataset may have affected the results. The work will be implemented in real time and also will be evaluated using some other banking or credit card dataset.

REFERENCE

1. http://www.thehindu.com/business/Economy/over25800onlinebankingfraudcasesreportedin2017saysgovernment/article22327229.ece.
2. P. Gühring, "Concepts against man-in-the-browser attacks," Update, vol. 2006, pp. 9–12, 2006.
3. N. Falliere and E. Chien, "Zeus: King of the Bots," Symantec Secure. Response (http//bit. ly/ …, no. November, pp. 1–14, 2009.
4. https://krebsonsecurity.com/tag/gameover-zeus/.
5. IOActive, "Reversal and Analysis of Zeus and SpyEye Banking Trojans," IOActive, Inc Tech. White Pap., no. 866, 2012.
6. Marc Fossi,"Banking with Confidence", Symantec Official Blog 2008.
7. Matt Liebowitz, "Tiny 'Tinba' Banking Trojan Is Big Trouble", msnbc.com, 2012.
8. Anton Cherepanov, Robert Lipovsky, "HESPERBOT-A New, Advanced Banking Trojan in the Wild", White paper, 2013.
9. P. Black, I. Gondal, and R. Layton, "A survey of similarities in banking malware behaviors," Comput. Secur., 2017.
10. RSA, "Making Sense of Man-In-The-Browser Attacks: Threat Analysis and Mitigation for Financial Institutions," RSA White Pap., 2010.
11. S. Kovach and W. Ruggiero, "Online banking fraud detection based on local and global behavior," ICDS 2011, Fifth Int. Conf. Digit. Soc., no. c, pp. 166–171, 2011.
12. Kancherla R., Venkata R., Verma A., "Behavioral Fraud Mitigation through Trend Offsets", Genpact India, (2008).
13. S. Alimolaei, "An intelligent system for user behavior detection in Internet Banking," 2015 4th Iran. Jt. Congr. Fuzzy Intell. Syst., pp. 1–5, 2015.
14. L. Fang, M. Cai, H. Fu, J. Dong,"Ontology-Based Fraud Detection",Computational Science ICCS (pp.1048-1055). Springer (2007).
15. Carminati M, et al., BANK SEALER: A decision support system for online banking fraud analysis and investigation, Computers & Security (2015).