Web Security System based on Human Immune System

Rashmi Bangar
M.Tech, Department of Computer Science & Engineering,
Godutai Engineering College for Women
Kalaburagi, India

Mangala S. Biradar
Professor, Department of Computer Science & Engineering,
Godutai Engineering College for Women
Kalaburagi, India

ABSTRACT
The Web Hacking Database, for short, is a Web Application Security Project dedicated to maintaining a list of web applications related security incidents. The goal is to serve as a tool for raising awareness of the web application security problem and provide information for statistical analysis of web applications security incidents. However to understand the risk associated with web hacks, we need to fully understand the likelihood and the impact of the attacks, and not just the technical details. To overcome this we have develop this application .here we using human immune system. By using functionality of dentritic cell and danger theory

1. INTRODUCTION
Nowadays, the World Wide Web (WWW) plays an important role in human life. Web applications are becoming increasingly popular in all aspects of human activities; ranging from science and business to entertainments [1]. Consequently, web servers and web application are becoming the major targets of many attacks. Due to the growing number of computer crimes, needs for techniques that can secure and protect web servers and web applications against malicious attacks have been highlighted. Unfortunately, current security solutions, operating at network and transport layers, have insufficient capabilities in providing acceptable level of protection against web-based attacks.

A dynamically monitors the input requests to the web server in order to decide whether a given set of requests is indicative of an attack or represents a normal web surfing activity As the web servers record all the requests processed by them in access log files, these files could be considered as a major source of information that can be analyzed

Forrest et al. [2] introduced use of computer immunology to protect the computer systems using the principles of human immune systems. In these paper we using system like artificial immune system (AIS) as applied to web security [3].primary function of immune system is protect body from antigen. Main fuction is It has great pattern recognition capability that may be used to distinguish between foreign cells entering the body (non-self or antigen) and the body cells (self)[4].

The objective of this paper is to propose a a immune model for anomaly detection by taking inspiration from the Danger Theory (DT) in Human Immune System (HIS)[5]. In 1994, a hotly debated hypothesis in immunology, known as the Danger Theory (DT) illustrated that the HIS can detect danger in additional to the collection of proteins known as antigens in order to trigger appropriate immune responses[5][6]. In 2005, Kim et al[8] introduced the theory to detect worms.

For anomaly detection Greensmith et al. [7], [8]proposed the Dendritic Cell Algorithm (DCA) whose purpose is to correlate data in the form of antigens and signals, then to identify groups of antigens as normal or anomalous. The algorithm performs multi-sensor data fusion and correlation which results in a ‘context aware’ detection system.

The DCA is a multi-sensor data fusion and correlation algorithm, which can perform anomaly detection on ordered datasets, including real-time and time- series data. The signal fusion process is inspired by the interaction between

DCs and their environment[7]. Dendritic cells (DCs), part of the innate immune system and an important antigen presenting cell, interact with antigens collected front issue and perform the role of coordinating T cell based immune responses, both reactive and for generating tolerance.[5]

2. BACKGROUND
2.1 Human Immune System (HIS)
Human immune system is system of biological network of cell n tissues .It protect the body against the viruces and diseases[1].it consistence of many cell of combination which play important role in body[2].antigen identified by immune system. Which cell are harmless to body are called self. Which causes diseases are called by nonself. The B-cells and T-cells are the part of the adaptive system; they are responsible to detect unknown pathogens B cell will make an antibody that blocks a virus that causes the common cold, while another produces an antibody that attacks a bacterium that causes pneumonia [9].T cell works in two way direct and regulate immune response; other direct attack infected cell.Negative selection are used for the identify the self cell[10].

It is difficult to give picture of such a complex system.

2.1.1 Dendritic Cells
- Dendritic cells patrol our bodies to see if there is anything we should activate our immune system against
- They are very important in regulating our immune system

DCs are the first defense line for HISs which will arrive at the locations where antigens intrude . These pieces will be attached to APCs and presented to the T-cells. DCs can be regarded as the commanders for HIS; they can combine the danger and safe signal information to decide if the tissue environment is in distress or is functioning normally. DCs are sensitive to two classes of molecule namely PAMPs and 'safe' signals.DC produce its own output signals it relatively depended on the input signals [1]. If collected antigen are from danger and PAMP environment it called as ‘anomalous’.

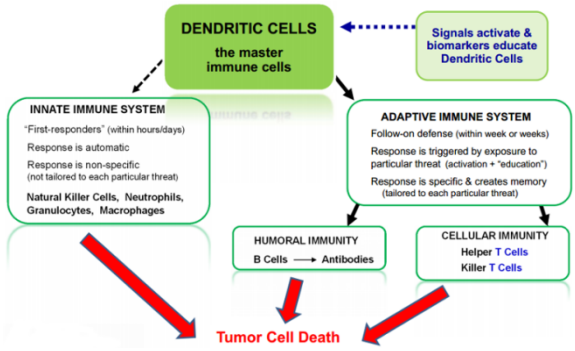


Fig 1: Working of Dentritic Cell

2.1.2 T-CellT

Cells kills antigens or help in the development of B-cells[6].T cells are divided to immune responce in two major ways: some direct and regulate immune responses; others directly attack infected or cancerous cells.Dc cells inspire to T cell to react to the antigen in popper manner. Both B-cells and T-cells continuously circulate around body in the blood and encounter antigens for activation and evolution. T cells only recognize an antigen if it is carried on the surface of a cell by one of the body's own MHC, or major histocompatibility complex, molecules on the surface of the DCsn will show the degree of the danger cells[11].killer T cells are directly attack other cells carrying certain foreign or abnormal molecules on their surfaces.

2.1.3 Artificial Immune Systems

Artificial Immune Systems (AIS), which is based on HIS, have been applied to anomaly detections [12][13][14][5][15]. AISs have been developed according to negative selection algorithm and clonal selection algorithm which are based on the classical self-nonself theory; nonselfs are entities which are not part of human organisms. This so-called self-nonself classification theory had been challenged while failing to explain several immunological phenomena. Some alternative theories have been proposed, for example, the danger theory (DT). DT postulates that the human immune systems respond to the presence of molecules known as danger signals, which are released as results of unnatural cell deaths.

2.1.4 Danger Theory (DT)

Matzinger [7] proposed the Danger Theory, which has become more popular among immunologists in recent years for the development of peripheral tolerance (tolerance to agents outside of the host There are two phase of danger theory activation and suppression. when the danger single activated immune system activated. The suppression arises as the cell death. [2] DT proposes that APCs, (in particular, DCs), have danger signal receptors (DSR) which recognize signals sent out by distressed or damaged cells.APCs are activated via the danger signals. These activated APCs will be able to provide the necessary signals to the Tcells (more precisely, T-helper cells) which control the adaptive immune response. Danger signals are generated by ordinary cells of the body that have been injured due to attacks by pathogens. Because of this signals there are 3mode of operation: immature, semi mature, mature. In immature it collects the information about antigens with safe and danger signals from the environment [18].[16].when it become safe it become semi-mature state.if it is dangerous,it converted to mature state.

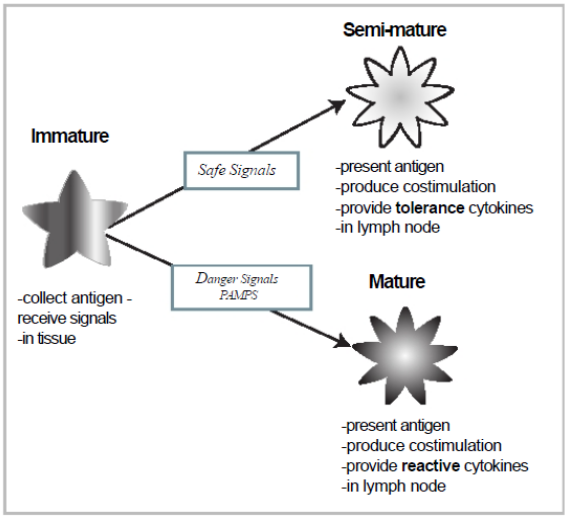
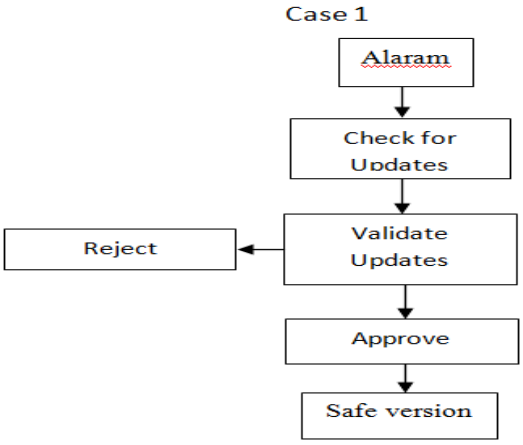


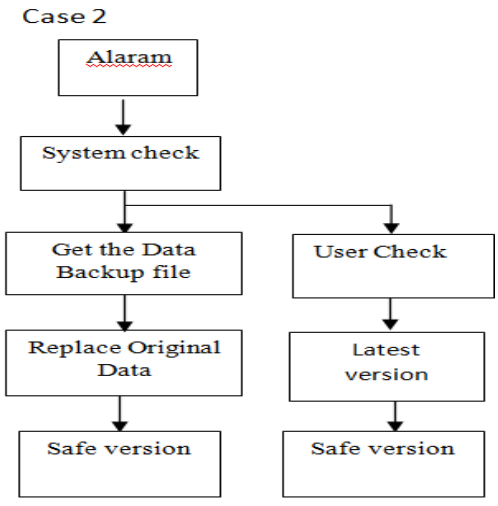
Fig 2: Working of Danger Theory

3. IMMUNE SYSTEM APPLIED TO WEB SECURITY

CASE 1: Normal Case



CASE 2: Danger Case



Here in Case 1, the admin waits and check for the updates, if found then validates the user requested data. If the data is correct then the same data is pushed to prod by admin approving the changes else it will be rejected.

In Case 2, the system will try to stop the attack once there is a alaram in system detecting the hack. Once the Malicious Detection is detected by invalid IP Address, the system will track the DB by finding the DB backup and replaces with older data, if on backup file found then it will request user to update the data once again from user end.

This paper just works as same as Immune system. The main agenda of Immune systems is to take care of Immune and keep it healthy and working condition all the time. Here our website behavior is also as same as the immune system.

In Immune, there'll be Virus, Bacteria, Fungus and Parasites threads, each and every threads has its own functionality which affects to body immune system. Even in our web project we have lots attacks or threads which targets our database such as SQL injection, Cross site scripting (XSS), Cross site request forgery (CSRF), Man in the middle etc. Each and every thread has its own functionality which affects Database as in Immune system.

Example, in Immune system if there's virus thread occurred in nose and takes our body cells the person can feel sick. In same way our application might get attacked by Hackers and attack the database.. To avoid this, there're various steps can be taken. As Immune system, in the same way, our web algorithm Identify the hack which parts the hack is took place, is it header part or is it in body or in footer. It identifies and takes necessary action.

In Immune systems there are various backup cells which attack against the virus /threads. In our web projects we do have DB backup each and every time. Taking this DB Backup file, our algorithm finds the effected part and reflects the same in view page. The user/admin can rollback with original data, stopping the thread/attack keeping safe and secure entire web application system.

Algorithm

input: signals from external ip address

Output: DB context (0 for safe/1 for danger)

initialised (Immature state);

while Accessed IP Address *!= Allocated IP Address*

DB context is assigned as 1;

State of DC agent i=”mature”;

Get DB Backup file;

If (file not found) then

Request user to update the data

Else

Comparison done;

get signals;

calculate interim output signals;

update the backup file;

DB context is assigned as 0;

State of DC agent i=”semi-mature”;

End if

End

Data location update to table;

Kill Cell;

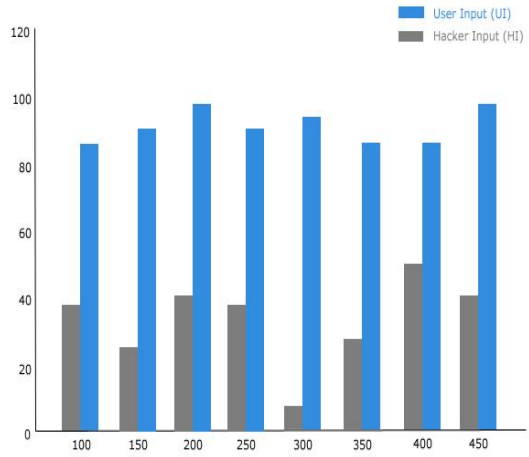
This Algorithm is inspirited by Dendritic Cell Algorithm which works as human immune system. As human system recognize the danger signal and reacts on that, our project also works as same as human system. The above algorithm explains the implementation of our project.

In above algorithm, it first detects the danger signal via invalid IP address. If found that there's invalid IP address trying to access the web page database, DB context is assigned as 1 and DC agent i is assigned to "mature" which means the DC agents is in danger. Once the DC agents are in danger it will try to get the backup file of database, if not found then requests user to update the data once again. If found then then gets signal and comparison with backup file and reverts the data back assigning DB Context to 0 and state of DC agent i as "semi-mature". Now the DC agent is again in normal state.

Our system ensures that it will keep track of process all the time, if any issue it takes the action immediately making sure that the system is in good health all the time.

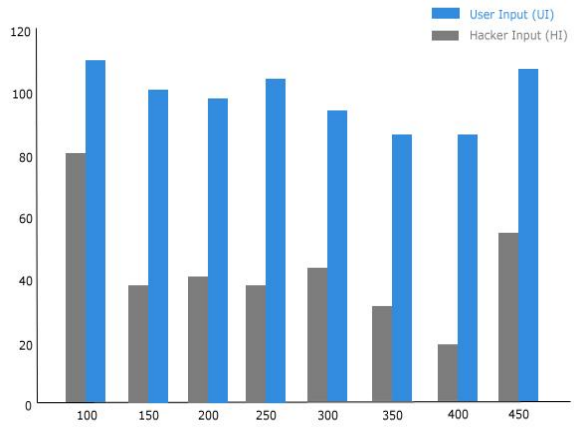
4. RESULT AND ANALYSIS

4.1 Comparison of True Positive



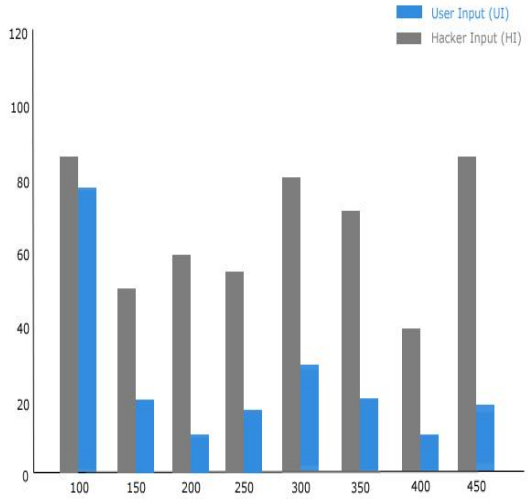
The comparison of true positive i.e, number of attacks detected when malicious input is applied to the application is shown in above figure. In this case the UI and HI, the figure shows that average detected in the case of UI is 65% and HI of 10%. The values highlighted in blue makes a good choice for number of epochs.

4.2 Comparison of True Negative



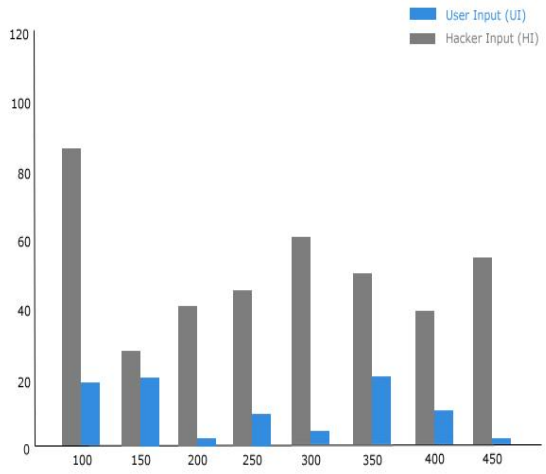
The comparison of true negative i.e, number of valid inputs detected when valid input is supplied to the application is show in above figure. The result shows that system performs better in detection of valid input compared to Hackers Input. The average detection of UI in case of True Negative is of 77% that of HI is 32%.

4.3 Comparison of False Positive



The comparison of false positive i.e, number of valid input not detected when valid input is applied to application is shown in above figure. The this case of UI and HI, the result shows that UI result is reduced rate of non-detection of valid input compared to HI. The average number of valid inputs not detected in the case of UI is 22% in that of HI 48%.

Comparison of False Negative:



The comparison of false negative i.e, number of attack not detected when malicious input is supplied to the application is show in above figure. In this case of UI and HI. The result shows that UI result is reduced rate of non-detected of malicious input compared to HI. The average number of attacks not detected in case of UI is 8% and that of HI 44%.

5. CONCLUSIONS AND FUTURE WORK

The main goal of this research was designing a host-based and protects it from hackers. Finally, we proposed the use of a novel algorithm, inspired by the natural immune system, in order to produce a set of detectors that can cover the space of non-self (attack) properly and match to the non-self data and detect them. The results presented in this paper, proved the high ability of the proposed algorithm in detecting abnormal activities compared to some well-know and classical learning algorithms. The most significant improvement that can lead to fruitful this research in future is to prepare the system to perform in an online state.

6. REFERENCES

[1] Iman Khalkhali, Reza Azmi, Mozhgan Azimpour-Kivi and Mohammad Khansari ," Host-based Web Anomaly Intrusion Detection System, an Artificial Immune System Approach"in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011

[2] F. Gu, U. Aickelin, and J. Greensmith, "An agent-based classification model," in *9th European Agent Systems Summer School (EASSS2007)*,2007.

[3] P. Harmer, P. Williams, G. Gunsch, and G. Lamont, "An artificial immune system architecture for computer security applications," *IEEE Transactions on Evolutionary Computations*, vol. 65, no. 3, pp. 252–280, November 2002.

[4] 1J.R. Al-Enezi, 1M.F. Abbod & 2S. Alsharhan," Artificial Immune Systems – Models, Algorithms And Applications,"Ijrras 3 (2) , May 2010.

[5] J. Zhang and Y. Liang, "Integrating innate and adaptive immunity for worm detection," in *Proceedings of the Second International Workshop on Knowledge Discovery and Data Mining*, 2009, pp. 693–696.

[6] Matzinger. P, (1994) "Tolerance, Danger and the Extended Family,"*Annual Review in Immunology*, vol.12, 2004, pp. 991-1045.

[7] J. GreensmithU, Aickelin, and S. Cayzer, "Detecting danger: The dendritic cell algorithm," *Robust Intelligent Systems*, vol. 12, pp. 89–112, 2008.

[8] U. Aickelin, P. Bentley, S. Cayzer, and J. Kim, "Danger theory: The link between ais and ids," *Lecture Notes in Computer Sciences*, vol. 2787, pp. 144–165, 2003.

[9] L. N. de Castro and J. Timmis,"Artificial Immune Systems:A Novel Paradigm to Pattern Recognition,"Computing Laboratory University of Kent at Canterbury.

[10] Antara Malakar and Tejbanta Singh Chingtham,"An Artificial Immune System For Humancomputer Interaction Through Speech,"International Journal of Instrumentation and Control Systems (IJICS) Vol.2, No.3, July 2012.

[11] Chung-Ming Ou,Yao-Tien Wang nad C.R.Ou,"Intrusion Detectuin System Adapted from Agent-bsed Artificial Immune System,"2011 IEEE

[12] International Conference on Fuzzy Sstems June 2011 27-30,2011,Taipei,Taiwan.

[13] F. Gu, U. Aickelin, and J. Greensmith, "An agent-based classification model," in *9th European Agent Systems Summer School (EASSS2007)*, 2007.

[14] U. Aickelin, P. Bentley, S. Cayzer, and J. Kim, "Danger theory: The link between ais and ids," *Lecture Notes in Computer Sciences*, vol. 2787, pp. 144–165, 2003.

[15] Kim, *An Artificial Immune System Architecture for*

Computer Security Applications. New York: John Wiley and Sons, 1978.

[16] H. Fu, X. Yuan, and N. Wang, "Multi-agents artificial immune system (maais) inspired by danger theory for anomaly detection," in *2007 International Conference on Computational Intelligence and Security Workshops*, 2007, pp. 570–573.

[17] S. Forrest, A. Hofmeyr, T. Somayaji, and Longstaff, "A sense of self for unix processes," in *Proceedinges of the 1996 IEEE Symposium on Research in Security and Privacy*, 1996, p. 120V128.

[18] J. Greensmith, U. Aickelin, and G. Tedesco, "Information fusion for anomaly detection with the dendritic cell algorithm." *Information Fusion*, vol.11, no.1, pp.21–34,2010.