

- [26] S. Aksoy, "Introduction to Pattern Recognition Part I," *Pattern Recognit.*, pp. 1–26, 2005.
- [27] S. Aksoy, "Introduction to Pattern Recognition Human Perception," *Pattern Recognit.*, pp. 1–40, 2016.
- [28] J. Liu, J. Sun, and S. Wang, "Pattern Recognition : An overview," *Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 6, pp. 57–61, 2006.
- [29] S. Asht, R. Dass, A. Fallis, T. Y. Dn, T. Yyepg, E. Cambria, G.-B. Huang, L. L. C. Kasun, H. Zhou, C. M. Vong, J. Lin, J. Yin, Z. Cai, Q. Liu, K. Li, V. C. M. Leung, L. Feng, Y.-S. Ong, M.-H. Lim, A. Akusok, A. Lendasse, F. Corona, R. Nian, Y. Miche, P. Gastaldo, R. Zunino, S. Decherchi, X. Yang, K. Mao, B.-S. Oh, J. Jeon, K.-A. Toh, A. B. J. Teoh, J. Kim, H. Yu, Y. Chen, and J. Liu, "Pattern Recognition Techniques: A Review," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.
- [30] T. Slivka, "Pattern Recognition," *Pattern Recognit. Lett.*, no. November, pp. 1–11, 2010. [31] K.-S. Fu and A. Rosenfeld, "Pattern recognition," *Ieee Trans. Comput.*, vol. C-25, no. 12, p. 1336, 2006.
- [32] N. J. Nilsson, "Introduction to Machine Learning," *Mach. Learn.*, vol. 56, no. 2, pp. 387–99, 2005.
- [33] W. Is and I. Good, "Image Analysis and Pattern Recognition 1," *Canada Cent. Remote Sens.*, pp. 1–7, 2015.
- [34] M. Kumar, "A Real-Time Vehicle License Plate Recognition (LPR) System," *Dissertation*, no. July, p. 77, 2009.
- [35] L. Angeline, H. K. Lau, B. K. Ghosh, H. H. Goh, and K. T. Kin Teo, "Development of a License Plate Recognition System for a Non-ideal Environment," *Int. J. Simul. Syst. Sci. Technol.*, vol. 13, no. 3 C, pp. 26–33, 2012.
- [36] David João Adão dos Santos, "Automatic Vehicle Recognition System- An approach using car rear views and backlights shape," *Dissertation*, no. September, 2008.
- [37] S. Saha, S. Basu, M. Nasipuri, and D. K. Basu, "Development of an automated Red Light Violation Detection System (RLVDs) for Indian vehicles," *Natl. Conf. Comput. Commun. Syst.*, no. March 2016, pp. 59–64, 2009.
- [38] L. Kodwani, "Automatic Vehicle Detection, Tracking and Recognition of License Plate in Real Time Videos," *Master Thesis*, 2013.
- [39] S. Ozbay and E. Ercelebi, "Automatic vehicle identification by plate recognition," *World Acad. Sci. Eng.*, pp. 222–225, 2005. [40] G. Garg and A. Kaur, "Study of Various Vehicle Detection Techniques –A Review," *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 2, no. 3, pp. 1–5, 2016.
- [41] E. C. Sharma and E. A. Singh, "An Efficient Approach for Detection and Extraction of Vehicle License Plates using Edge Detection Technique," *Int. J. Comput. Sci.*, vol. 5, no. 1, pp. 33–36, 2014.
- [42] A. Mogelmose, D. Liu, and M. M. Trivedi, "Detection of U.S. Traffic Signs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 3116–3125, 2015.
- [43] A. Mogelmose, M. M. Trivedi, T. B. Moeslund, Ieee, and A. Mogelmose, "Traffic Sign Detection and Analysis: Recent Studies and Emerging Trends," *2012 15th Int. Ieee Conf. Intell. Transp. Syst.*, pp. 1310–1314, 2012.
- [44] M. S. Kristoffersen, J. V. Dueholm, R. K. Satzoda, M. M. Trivedi, A. Mogelmose, and T. B. Moeslund, "Towards Semantic Understanding of Surrounding Vehicular Maneuvers: A Panoramic Vision-Based Framework for Real-World Highway Studies," *Traffic Technol. Int.*, pp. 1–8, 2014.
- [45] S. Hosseinyalmdary, A. Yilmaz, C. Section, and H. Transformation, "Traffic Light Detection Using Conic Section Geometry," *Photogramm. Comput. Vis. Lab.*, pp. 1–10, 2011.
- [46] M. L. Ginsberg and G. I. Road, "Traffic Signals and Autonomous Vehicles: Vision-based or a V2I Approach?," pp. 1–11, 2015.
- [47] A. Prioletti, A. Mogelmose, P. Grisleri, M. M. Trivedi, A. Broggi, and T. B. Moeslund, "Part-based pedestrian detection and featurebased tracking for driver assistance: Real-time, robust algorithms, and evaluation," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 3, pp. 1346–1359, 2013.
- [48] M. P. Philipsen, M. B. Jensen, A. Mogelmose, T. B. Moeslund, and M. M. Trivedi, "Learning Based Traffic Light Detection: Evaluation on Challenging Dataset," *18th Intell. Transp. Syst. Conf.*, no. Submitted, pp. 1–5, 2015.
- [49] M. P. Philipsen, M. B. Jensen, R. K. Satzoda, M. M. Trivedi, A. Mogelmose, and T. B. Moeslund, "Day and Night-Time Drive Analysis using Stereo Vision for Naturalistic Driving Studies," *IEEE Intell. Veh. Symp.*, vol. 2015, no. June, pp. 1–6, 2015. [50] L. Angeline, K. T. Teo, and F. Wong, "Smearing Algorithm for Vehicle Parking Management System," *Proc. 2nd Semin. Eng. Inf. Technol.*, no. July, pp. 331–337, 2009.
- [51] a. Akoum, "A New Algorithmic Approach for Detection and Identification of Vehicle Plate Numbers," *J. Softw. Eng. Appl.*, vol. 3, no. 2, pp. 99–108, 2010.
- [52] H. Ri, H. Z. Qhxudo, Q. Lpdjh, S. Olfhqvh, S. Uhfrjql, and H. U. V Vwhp, "Recognition of Car License Plates using a neocognitron type of Artificial Neural Network," pp. 1–12, 2015.
- [53] P. Vijayalakshmi, "Design of Algorithm for Vehicle Identification by Number Plate Recognition," *Engineering*, 2012.
- [54] M. A. Joarder, K. Mahmud, T. Ahmed, M. Kawser, and B. Ahamed, "Bangla Automatic Number Plate Recognition System using Artificial Neural Network," *Asian Trans. Sci. Technol. (ATST)*, vol. 2, no. 1, pp. 1–10, 2012. [55] K. Bora, "Car Plate Recognition," *Dissertation*, no. June, 2009.

On the Relationship between Human Immunology and Computer Immunology

Salau-Ibrahim Taofeekat Tosin
Department of Physical Sciences, computer Science Unit
Al-Hikmah University
Ilorin, Nigeria
taofeekatsalau@gmail.com, ttsalau@alhikmah.edu.ng

Jimoh Rasheed Gbenga
Faculty of Communication and Information Science
University of Ilorin
Ilorin, Nigeria
Jimoh_rasheed@yahoo.com

Yusuf-Asaju Ayisat Wuraola
Faculty of Communication and Information Science
University of Ilorin
Ilorin,
ayisatwuraola@gmail.com

Nigeria

Abstract— In this conceptual paper, the features of computer and human immunology were described with subtle emphasis on computer virus. As would be argued, both are related since the human immunology has been an inspiration for building more secured, stronger computer systems and interconnection between them over the years. It is expected that the conceptual framework would not only expose researchers to the basics of biological immune system, but also to computer security architectures that can borrow ideas from it. Review of related research in human and computer immunology was used.

Keywords—Immunology, Human virus, Computer virus

I. INTRODUCTION

In recent times, relationship between computer and human immunology has been the focus of several academic researchers[1]–[3]. This has been in a bid to develop computer information systems that can withstand exposure to increasing dynamic nature of intrusions just like pathogens do in human beings. Human immunology deals with the study of how the body fights against as well as protects itself from bacteria, viruses, protozoa and fungi collectively known as pathogens. This process in the human body is highly coordinated and proven to protect the human body to a large extent despite the constant exposure to these pathogens. Similarly, there are protective mechanisms such as intrusion detection and prevention systems used in computer systems to guard against intrusions. For instance, viruses, worms, Trojans, ping of death, denial of service, penetration attempt and reconnaissance[4].

Globally, every sector of the economy such as government, education, military and financial sector now relies heavily on internet technology to carry out operational and managerial duties. The most alarming part is that threats to the information system assets are increasing geometrically[5]. A recent survey conducted by Cybersecurity Nexus in 2015 revealed that 77% of respondents reported an increase in cyber-related attacks in 2014 compared to the preceding year [6]. In the same survey, 82%

opined there would be more attacks in the succeeding year [6]. Also, the report for 2015 revealed that organisations may experience an increased negative impact of cyberattack by 2016[7]. In Nigeria, the use of internet has increased tremendously to 51.1 % as at June 2015 as against 26.5% in 2011[8]. Therefore, seeking inspiration from the defense mechanism of biological organism would be worthwhile since it protects the body effectively against known and new invasions. The use of biological analogies collectively termed computational intelligence is not new to this study. As a result, this present study is one of the earliest study to vividly describe the relationship between human virus and computer virus under the umbrella of human and computer immunology. Detailed review of past studies would be employed. The rest of this paper provides a brief description of human immunology, computer virus and computer immunology. Finally, requirements necessary for designing a computer immune system and possible computer security architectures that can benefit from computer immunology will also be discussed.

II. HUMAN IMMUNOLOGY

The human immune system is a group of cells, molecules, tissues, organs and circulatory systems[9]. The immune system cells are created in the thymus or bone marrow as the case may be. The human body is constantly exposed to pathogens such as virus which is the focus of this study. The body's function is to detect and remove such virus from the body and ensure that new or same virus does not get into the body subsequently [10]. The Human immune system is multilayered in nature, see Fig 1. The layers are made up of physical barriers, physiologic barriers, the innate immune system and adaptive immune system[11], [12]. The physical barrier, for instance, skin and mucous membrane, is the first contact for virus. The physiologic barrier on the other

hand, are saliva, sweat and tears. These fluids have varying pH and temperature as well as contain enzymes that

make the environment unconducive for thriving. Next is the innate and adaptive immune system s which act on any virus es that evade the first two layers. Moreover, the adaptive immune system is divided into humoral immunity and cell mediated immunity [13]. The innate and adaptive immunity have cells that make it function effectively, see Fig 2.

A. Innate Immune System

Innate immune system is a form of human immune system that uses a set of receptors called Pattern Recognition Receptors (PRRs)[12]. They recognize molecule s specific to pathogens called Pattern

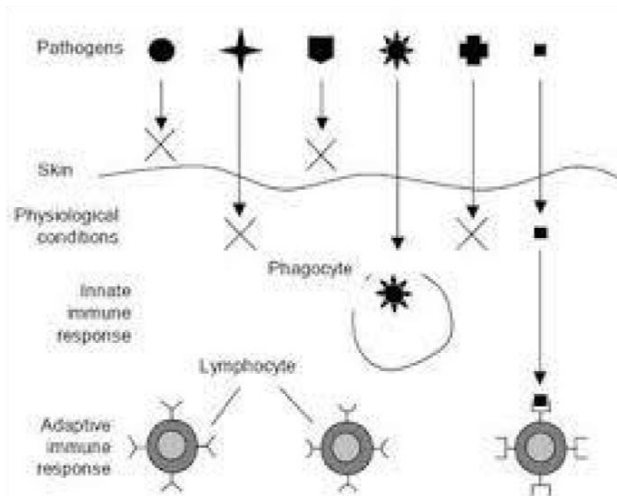


Fig. 1 Layers of Human Immune System [14]

Recognition Receptors (PRRs)[12]. They recognize molecules specific to pathogens called Pathogen Associated Molecular Patterns (PAMPs). This recognition indicates the presence of pathogen in the body. The role of the innate immune system is to defend the host at the onset of infection which is achieved by non-specific recognition of the pathogen. Secondly, it helps to induce the adaptive immune system. Thirdly, the innate immune system determines the type of adaptive response through the expression of co-stimulatory signals in Antigen presenting cells (APCs).

B. Adaptive Immune System

Pathogens that are not destroyed by the innate immune layer get to the adaptive immune layer. This part of the immune system uses complex learning process to achieve better immunity of the human body [11]. Generally, T-cells and Bcells are the lymphocytes used to protect the body. The protection is achieved by using somatically generated antigen receptors clonally distributed on the lymphocytes. This leads to specific recognition of pathogen leading to pathogen-specific long term memory [9]. The receptors used by the adaptive immune system are T-cell receptors (TCR) and B-cell receptors (BCR). Also, the adaptive immune system enables response to pathogen that the body has never encountered before. While Bcell aids production

adaptive immune system.

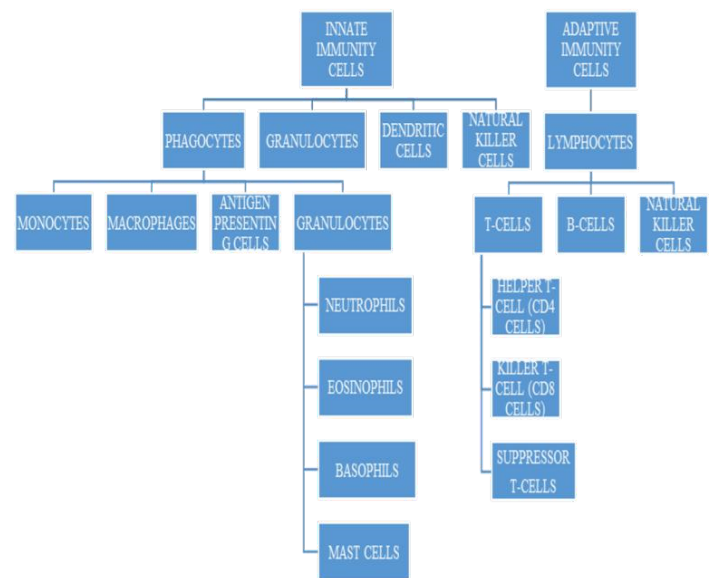


Fig. 2 Cells of the Innate and Adaptive Immune System

III. HOW IMMUNE SYSTEM PROTECTS THE BODY FROM PATHOGENS

The pathogen on getting into the body produces antigen (Ag). Antigen is a foreign molecule from pathogen or other exogenous element. Therefore, the target of all processing in and secretion of antibodies in response to exogenous elements, T-cells attacks infectious cells and control other cell activities in the body [12]. Table 1. give a summary of the major differences between the innate immune system and the human immune system is directed towards destroying the antigen and maintaining the human body.

The first point of contact by the antigens are phagocytes such as macrophages. Macrophages move freely in the body to digest antigens they encountered. Afterwards, the antigens are fragmented into antigenic peptides [12]. Then, the fragments of the antigenic peptides bind to major histocompatibility complex

(MHC) molecules. The antigenic peptide-MHC molecules combination is displayed on the surface of the cell. Next, receptors present on T lymphocyte (T-cell) and B lymphocyte (B-cell) recognize the antigenic peptides – MHC molecule and get activated [13]. T-cells on activation divide and secrete lymphokines (chemical signals) that activate other components of the HIS. Conversely, B-cells on activation respond to the Tcell lymphokines. B-cells have an additional ability of recognizing antigenic peptides that do not bind to MHC molecules. In the same way, B-cells get activated after the recognition process, divide and secrete antibody proteins. These antibody proteins can defuse as well as trigger the destruction of the antigens. Finally, memory cells are developed from the T and B cells which aid elimination of the same antigen if presented in future. As a result, the human immune system is enhanced. More details of how the body is protected can be found in [10].

Table 1. Differences Between Innate Immune System and Adaptive Immune System

Innate Immune System	Adaptive Immune System
First line of defense	Second line of defense
Evolves and passes from one generation to another	It is an acquired immune system
Response to pathogens is usually within few hours	Response to pathogens takes days or months due to clonal selection of T-cell and B-cell
Referred to as non-specific immunity	Referred to as antigenspecific immunity
The receptors are Pathogen Recognition Receptors (PRR)	The receptors are T-cell (TCR) and B-cell (BCR) receptors

IV. COMPUTER VIRUS

Adleman in 1987 invented the term computer virus [15]. Computer virus, like its biological counterpart human virus, appends parasitically to existing programs in order to attack the resources and create more copies of the virus [16]. When this happens, the host system fails. Subsequently, when virus enters a computer system, it gets executed by the user of the computer system. Afterwards, the virus searches for programs the user has access to and appends itself to the program. Control is

immediately returned to the original program, therefore, the user may not notice that another program on the computer system has been infected. As a result, the copy of the virus already in the system gets replicated and spread across the computer system by residing in the memory, in order to monitor system activity. Due to the increasing use of the internet, infected programs are easily transferred to other computer systems electronically.

Most times, computer viruses occur in form of malicious code. The common types of malicious codes are Trojan horse, worms and viruses. Also, the payload contents of these codes generally cause damage [17]. Trojan is a program that disguises as a legitimate program by taking the same name but performs different functions. This similar nomenclature makes it easier for user to mistakenly execute the Trojan. When executed, the intruder circumvents the entry security mechanisms of the computer system. Worms on the other hand execute independently and require a computer network to proliferate. Lapses in network and communication protocol aid their actions. Fig. 3 shows the taxonomy of computer virus. Computer viruses are detected with the use of anti-virus software by employing activity monitors and integrity management systems techniques [15]. The former notify users when system activity associated with viruses occur while the latter warn user when unusual changes are made to files. When a new virus is detected, human experts study and analyze the virus in order to determine the behavior and how it appends itself to the host program. Sequences of instructions present in the virus are collated into signatures that are encoded into the anti-virus software. Analyzing viruses is a difficult and time consuming task that leads to inefficient signatures and consequently high rate of false positives.

According to Harmer [17], virus can also be detected in four different ways which are Appearance, behavior, change and bait. To detect virus by appearance, pattern matching is utilized between scan string and the infected entity. Scan string is the signature made up of sequence of instructions present in the virus. This is used for recognition of the virus in subsequent attacks. As for behavior, the operations performed by the virus is monitored. Moreover, viral activities are similar to normal system operations. Therefore, the antivirus system has to be able to distinguish suspicious activities from normal activities.

When virus gets into the computer system, it infects the host and multiply. This results in changes in the host system. Therefore, it is possible to detect virus by observing the changes in the host. Changes can be easily noticed in the initial state of file. Such changes are file size and file date. Another method is the bait method in which a dummy file usually a replica of file on the computer system is placed in directories or named with file extension prone to virus attack. Such file is also programmed to behave in a virus attractive manner. For instance, executing frequent read and write operations. Afterwards, the original dummy file state is saved and monitored for changes. Occurrence of changes signifies the presence of virus in the computer system. Detailed information regarding the strengths and weaknesses of the detection methods can be found in [17]. The relationship between human virus and computer virus is

shown in Table 2 and indicated a compelling reason that supports close analogy between computer virus and human virus.

Table 2. Relationship between Human Virus and Computer Virus

Human Virus	Computer Virus
DNA contains the definition of self	Program code contains a definition of self
Human virus multiply by reproducing its DNA	Computer Virus multiply by reproducing copy of its program code
Some human viruses attacks specific species	Some computer viruses attacks specific types operating systems
Some attack specific cells	Some attack specific system files. For instance EXE and COM
Not all viral illness in human show symptoms. For instance Hepatitis B virus can be asymptomatic	Also not all computer virus attack shows obvious signs.

Human virus has incubation period before manifestation. Example, Rabies virus has an incubation period up to 6 months	Likewise, some computer virus delays until their payload reaches certain threshold. Example, Michelango virus [17]
Human virus multiplies easily. For instance Human Immunodeficiency Virus (HIV)	Computer virus also makes copies of itself rapidly when it enters the computer system

Consequently, despite the fact that the use of generic antivirus software removes viruses from computer system, it has few drawbacks. First, it can only detect new viruses that have close sequence to existing viruses. Otherwise, it will be missed. Second, it detects virus only without removing it from the infected file. These two drawbacks necessitated borrowing ideas from the adaptive immune system in human immunology which is specific in its recognition of pathogens. Detection and response to viruses by adaptive immune system is apt such that new viruses can be detected easily. Therefore, designing a computer immune system would be worthwhile in order to alleviate the problems of generic anti-virus software. The next section is devoted for explaining computer immunology.

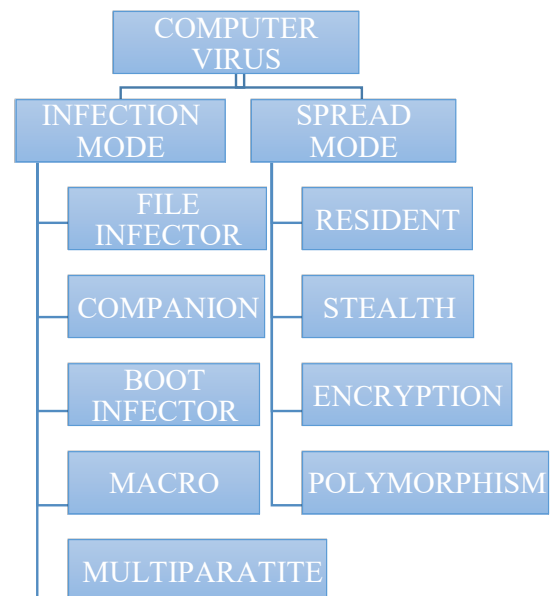


Fig 3. Taxonomy of Computer Virus [17]

V. COMPUTER IMMUNOLOGY

Human immunology and computer immunology are analogous from the security point of view. This is because both

ensure protection from invaders. Similar to the Human immune system, computer immune system must incorporate mechanisms from both the innate and adaptive immune system [18]. Human immunology has some desirable features that can be borrowed for improving the security of computer systems. The features according to Kim et al., [19], Ahmad [20] and Somayaji et al., [21] are: distributed, multi-layered, diversity, disposability, autonomy, adaptability, no secure layer, dynamically changing coverage, identity via behavior, anomaly detection, imperfect detection, noise tolerance, self-organizing and generation of antibodies. The listed properties serve as the basis for designing computer immune system for securing computer systems.

Building computer immune system involves certain steps as enumerated by Forrest et al., [2]. First, definition of self which involves defining what constitutes normal activities in a computer system. Detection, prevention and elimination of harmful abnormal activities is important. There should be a memory mechanism for previous intrusion as this aids protection against them when they reoccur. Ways of recognizing new intrusion must be put in place. Finally, protection of the computer immune system from self-attack.

Definition of self in the context of computer system can be normal memory access pattern, network traffic via a router, system call pattern, user behavior pattern, keyboard typing pattern as well as inward and outward flow of TCP/IP packet. Whereas, non-self or intrusions can be in form of misuse, reconnaissance, trojanization, scanning attack, penetration attacks, denial of service attacks and virus attacks. Works such as the one by Burgess explored computer immunology and led to the design of cfengine [1] and also the design of a Computer Virus Immune System (CVIS) by Harmer et al., [4] and Lamont et al., [22]. Extensive review on researches in this area can be found in [19], [23].

A. Computer Immune System Requirements

Kephart et al., [18] outlined the requirements of a computer immune system as innate immunity, adaptive immunity, delivery and dissemination, speed, scalability, safety and reliability, security and finally customer control. Innate immunity involves the ability to detect unknown viruses while adaptive immunity gives the computer immune system ability to automatically detect and remove previously known viruses from the computer system. The process of delivery and dissemination ensure the system successfully remove viruses on the infected host and also from other hosts in a networked environment. Speed allows the removal of viruses within limited period of time before they proliferate. Scalability is concerned with ability to maintain efficiency despite large volume of data. This is in two folds; scalability in virus analysis and updates. As for analysis, computer immune system must be able to handle virus analysis rapidly on one or several computers in a network. In addition, virus analysis must be updated frequently so that re-occurrence of the viruses can be tackled effectively to enhance adaptation. Safety and reliability guarantee low false positive rate as this ensures accuracy in detection. With security, it is important to ensure that scan string produced by the immune system for detecting viruses remain secured. Lastly, customers

must have control over the dissemination and delivery of scan string which can be manually or automated.

B. Potential Security architecture for Computer Immune System

This section describes computer security architectures that aid the concepts of computer immunology. Somayaji et al., [21], pointed out four possible architectures. Two additional architectures are added in this paper; heterogeneous and Mobile Ad-hoc Network.

1) Protecting Static Data

This involves protecting data on computer system from unauthorized access by computer viruses. In this architecture, virus- free data is regarded as self while virus- infected data is regarded as non-self. When compared to human immunology, it fits perfectly with the self-non-self-discrimination used for detecting virus and other anomaly in the human body. The mapping between the human components and computer system components is given in the Fig. 4 below.

Human cells	↔	Data
Pathogens	↔	Computer Virus
Self-cells	↔	Virus free data
Non-self-cells	↔	corrupt data

Fig. 4. Mapping Between Human Components and Computer Components

2) Protecting Active Processes

In this architecture, every active process is regarded as a cell. Also, passwords and file permission represent the skin and the innate immune layer respectively. The idea of lymphocyte can be factor in as “T-cell process”. Similar to the T-cell lymphocytes in the human body, T-cell process controls other processes and attack abnormal processes. For that reason, the T-cell process acts by slowing down, suspending, terminating or restarting the attacked process. Also, T-cell process undergoes negative selection in order to generate set of detectors. While some become memory detectors because they detect new intrusion. Moreover, adaptation to changes overtime is achieved by continuous generation of new detectors as well as adjusting their population via aging. See mapping in Fig. 5.

3) Protecting network of Computer

This consist of mutually trusting computers and mutually trusting disposable computers. For the first category, host-based and network-based security mechanism represent the innate immunity while lymphocyte processes i.e. T-cell processes represent the adaptive immunity. The distinguishing features of this architecture are that T-cell processes are mobile agents that serve as detectors. In addition, a computer is dedicated as the thymus. When implemented in a network, it can be used to protect the network and individual computers. In the second category, the main difference from all those discussed so far are

the computer components involved. Here, each computer in the network is the cell and the corresponding human component is the network of computers. Network defense mechanism serves

Self-cells	↔	Normal behaviour
Non-self-cells	↔	Abnormal behaviour
Cell	↔	Active process
Physical layer	↔	password
Innate layer	↔	File permission
Adaptive layer	↔	T-cell process
(Lymphocyte)		

Fig. 5. Mapping Between Human Components and Computer Components as the innate immunity while a set of lymphocyte machine serves as detectors in the adaptive immunity. The lymphocytes that are negatively selected monitor the computers in the network for the presence of intrusions. Entry of intrusion into the network either results in shutting down or rebooting the affected computer.

4) Protecting Heterogeneous Network

Heterogeneous network consists of computer and other devices with different operating system networked together. This network accommodates interworked architecture among different access network through internet protocol based platforms. This leads to the generation of several types of traffic with varying packet headers, varying MAC protocols and topologies [24]. This means attacks on such network can easily spread across the various access networks. This architecture closely resembles the complex nature of the Human body. Therefore, protecting such network can confidently use the security mechanism employed by the body against external attacks. For instance, individual network can be represented as cell while the whole heterogeneous network is regarded as the human body.

5) Protecting Mobile Ad-hoc Network (MANET)

Mobile Ad-hoc Network is self-organized group of wireless mobile devices (sensor nodes) without fixed infrastructure. Some of its features include but not limited to dynamic network topologies, complex application environment and limited physical security [25]. This type of network is susceptible to different types of security attacks such as viruses attack. Therefore, it is pertinent to provide secure communication for the network. [25]–[27] contains extensive review on Mobile Ad-hoc Network and its security challenges.

VI. CONCLUSION

The human immune system protects the body from pathogens such as viruses and their dangerous effects. This is achievable because of the various cells and mechanism present. Also, other features of the human immune system provide basis for its adoption in solving computer related problems especially computer virus attack. This paper presents the classification of computer viruses. It describes the requirements necessary to

design a computer immune system. Also, the relationship between human and computer immunology was presented. Furthermore, the computer security architectures that can benefit from the human immunology concept were explained.

REFERENCES

- [1] M. Burgess, "Computer Immunology," 1998, vol. 98, pp. 283–298.
- [2] S. Forrest, S. A. Hofmeyr, and A. Somayaji, "Computer immunology," *Commun. ACM*, vol. 40, no. 10, pp. 88–96, 1997.
- [3] P. Saurabh, B. Verma, and S. Sharma, "Biologically Inspired Computer Security System: The Way Ahead," in *Recent Trends in Computer Networks and Distributed Systems Security*, Springer, 2012, pp. 474–484.
- [4] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An artificial immune system architecture for computer security applications," *Evol. Comput. IEEE Trans.*, vol. 6, no. 3, pp. 252–280, 2002.
- [5] M. Jouini, L. B. A. Rabai, and A. Ben Aissa, "Classification of security threats in information systems," *Procedia Comput. Sci.*, vol. 32, pp. 489–496, 2014.
- [6] ISACA, "State of Cybersecurity: Implication for 2015," ISACA, USA, 2015.
- [7] ISACA, "State of Cybersecurity: Implications for 2016," ISACA, USA, 2016.
- [8] I. W. Stats, "Nigeria Internet Usage and Telecommunications Reports," *Internet World Stats*. 13-Aug-2016.
- [9] J. P. Twycross, *Integrated innate and adaptive artificial immune systems applied to process anomaly detection*. Citeseer, 2007.
- [10] C. A. Janeway Jr, "How the immune system recognizes invaders," *Sci. Am.*, vol. 269, no. 3, p. 72, 1993.
- [11] S. Amer, "Enhancing host based intrusion detection systems with danger theory of artificial immune systems," 2008.
- [12] L. N. De Castro and F. J. Von Zuben, "Artificial immune systems: Part I–basic theory and applications," *Univ. Estadual Campinas, Dezembro de, Tech. Rep.*, vol. 210, 1999.
- [13] U. Aickelin, D. Dasgupta, and F. Gu, "Artificial immune systems," in *Search Methodologies*, Springer, 2014, pp. 187–211.
- [14] L. N. De Castro and J. Timmis, *Artificial immune systems: a new computational intelligence approach*. Springer Science & Business Media, 2002.

- [15] J. O. Kephart, G. B. Sorkin, W. C. Arnold, D. M. Chess, G. J. Tesauro, S. R. White, and T. J. Watson, "Biologically inspired defenses against computer viruses," 1995, pp. 985–996.
- [16] T. M. Chen and J.-M. Robert, "The evolution of viruses and worms," *Stat. methods Comput. Secur.*, vol. 1, 2004.
- [17] P. K. Harmer, "A distributed agent architecture for a computer virus immune system," DTIC Document, 2000.
- [18] J. Kephart, G. Sorkin, M. Swimmer, and S. White, "Blueprint for a computer immune system," in *Artificial immune systems and their applications*, Springer, 1999, pp. 242–261.
- [19] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection—a review," *Nat. Comput.*, vol. 6, no. 4, pp. 413–466, 2007.
- [20] W. Ahmad, "Natural immune systems for developing novel Machine Learning algorithms," Auckland University of Technology, 2012.
- [21] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a computer immune system," 1998, pp. 75–82.
- [22] G. B. Lamont, R. E. Marmelstein, and D. A. Van Veldhuizen, "A distributed architecture for a selfadaptive computer virus immune system," 1999, pp. 167–184.
- [23] L. N. De Castro and F. J. Von Zuben, "Artificial immune systems: Part II—A survey of applications," *FEEC/Univ. Campinas, Campinas, Brazil*, 2000.
- [24] F. Hashim, K. S. Munasinghe, and A. Jamalipour, "On the negative selection and the danger theory inspired security for heterogeneous networks," *IEEE Wirel. Commun.*, vol. 19, no. 3, pp. 74–84, 2012.
- [25] L. E. Jim and M. A. Gregory, "A Review of Artificial Immune System Based Security Frameworks for MANET," *Int. J. Commun. Netw. Syst. Sci.*, vol. 9, no. 1, p. 1, 2016.
- [26] S. Ghanekar, N. Alrajei, and F. Mili, "Bio-Inspired Intrusion Detection for Wireless Sensor Networks," *Secur. Self-Organizing Networks MANET, WSN, WMN, VANET*, p. 347, 2016.
- [27] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.