Survey to Immune System and Internet of Things in Terms of Self-management

Shatha Habeeb
Department of Computer Sciences, University of Technology, Baghdad, Iraq
shathahabeeb@yahoo.com

Abstract

The rapid development in the world of Internet networks led to the emergence of Internet of things and Web of things which in turn requires speed and self-management for the success of the transmission of information and self-interaction between request and response to the latest event. In this research we clarify the similarity main points between the workflow of the immune system in humans, Artificial Immune Systems which work to protect the body from the strange things that enter the body and which require self-management and the Internet of things as an interconnected network consisting of a combination of things which permits communications between objects, machines and anything else with each other. IoT can be defined as a system comprised of things in the real world, these things are attached to sensors which are connected to the Internet through wired or wireless connection structure that requires self-management.

Keyword: Internet of things, web of things , self management , immune system, senser.

دراسة لنظام المناعة وإنترنت الأشياء من حيث الإدارة الذاتية

شذى حبيب

الجامعة التكنولوجيا – قسم علوم الحاسوب

الخلاصة

أدى التطور السريع في عالم شبكات الإنترنت إلى ظهور إنترنت الأشياء وويب الأشياء مما يتطلب بدوره السرعة والإدارة الذاتية لنجاح نقل المعلومات والتفاعل الذاتي بين الطلب والاستجابة لآخر حدث . في هذا البحث ، نوضح نقاط التشابه الرئيسية بين سير العمل في الجهاز المناعي عند البشر ، أنظمة المناعة الاصطناعية التي تعمل على حماية الجسم من الأشياء الغريبة التي تدخل الجسم والتي تتطلب الإدارة الذاتية وإنترنت الأشياء باعتبارها مترابطة شبكة تتكون من مجموعة من الأشياء التي تسمح بالاتصال بين الأشياء والآلات وأي شيء آخر مع بعضها البعض. يمكن تعريف إنترنت الأشياء كنظام يتكون من أشياء في العالم الحقيقي ، وترتبط هذه الأشياء بأجهزة استشعار متصلة بالإنترنت من خلال بنية اتصال سلكية أو لاسلكية تتطلب إدارة ذاتية.

الكلمات المفتاحية: انترنت الاشياء ، شبكت الاشياء ، الادارة الذاتية ، نظام المناعة ، اجهزة الاستشعار

1. Introduction

Involuntary computing is considered as model with self-managing (SM). This computing model observes the operating of computer's system and applications free of any human impact. Moreover, it becomes a significant strategic method which can be used to design easy-to-manage and reliable computer systems [1]. The function of SM is automating the whole process of error administration through automating the process of revelation, diagnosing and fixing these errors. The SM techniques guarantee the standalone of the error administration process with efficiency and reliability, Automatic computing or automatic management is applied in many areas in our real life or process [2].

The immune system in the human body defends itself spontaneously; the human body has the ability to differentiate between the inner cells and a group of atoms adhering together from the body of diseases, known as self and non-self, and protects the body. In the human body, the immune system protects the human body without any prior information of the attacker (bacteria) and its structure; On the other hand, Internet of things consists of a set of interconnected objects when connecting a sensor to detect the blaze in anywhere the fire is detected in the location of the sensor directly gives instructions to fire extinguishers to operate autonomously.

1- Related works

Several papers discussing compositions in different environments

In 2014, Jose Manuel Sanchez Vilchez, et al.[6] introduced a work titled "Self-healing Mechanisms for Software Defined Networks". The goal of this work is supplying SDN (Software Define Network) featured by means of error management via autonomic essential similar to self-healing techniques. The method suggested in this work is a public self-healing which depends on a Bayesian Networks for the diagnosis block, and it was utilized to a focus SDN infrastructure in order to establish its functions in case of flaws.

1- In 2016, Asghar, and Muhammad Zeeshan [7] introduced a work titled "Design and Evaluation of Self-Healing Solutions for Future Wireless Networks". This research deals with the process of founding inclusive and innovative solutions for the Self-Organizing Networks (SON) used to manage future wireless networks. More accurately, this work deals with one part of SON which is Self-Healing (SH). Errors can occur at some functional regions in a complicated cellular network. SH can be defined as autonomous error administration in wireless networks which comprise observing, diagnosing of errors and their reasons, triggering compensation, procedures of recovery, and evaluating the results.

2- Nicholas Wong et al., [8] (2012), made a proposal about the usage of AIS (Artificial Immune System) which imitates the technique of the immune systems in the humans in conserving the human body from the attacks with complex biological nature. The research deals with how using of AIS can be useful in an aspect of security management like revelation of credit card fraud. A case study is used to

explain the solution if any frauds happened in the transactions of credit cards in spite of the fact of using this mechanism in a wide range of applications in the field of E-business security.

3- R.Sridevi and Rajan Chattemvelli (2012) ,[9], proposed a combination method of artificial immune systems and genetic algorithm in order to detect the intrusion of network an ideal IDS system should be capable of evolving itself to identify not only known attacks but also unknown attacks. Algorithms depend on Genetic Engineering and Immune Systems are known to evolve and learn from small examples. In this paper it is proposed to investigate the efficacy of genetic search methods for feature selection and Immune system to classify threats and non-threats

2- Self-Managing

Self-managing can be defined as a process where the computer system can manage its functionality in the absence of human influence [21]. There are four functional fields in the system of autonomic computing: self-optimization, self-configuration, self-healing, and self-protection see figure1. The self- healing is a term called to every system or equipment has the facility to discover that it does not work properly without human influence. Moreover, it can do the required modifications to recover the error and back to its regular operation. Many users found that the cost of this service is very high, sometimes the cost is higher than the cost of the product itself, and for this reason, many developers -like IBM- introduce products that can repair themselves. This company is working on developing products that have self-configuring, self-optimizing, and self-protecting beside the property of self-healing as a part of the initiative of autonomic computing which has been adopted by IBM, and for this reason, IBM is using "self-managing" [22].

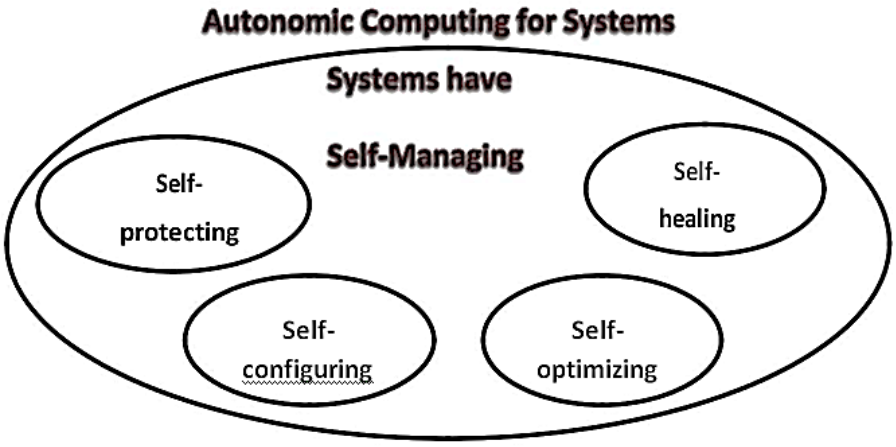

Figure (1) Self Managing System

There are several forms of the term "self-managing", which lead to special dimensions of control. The self-managing systems used in the initiative of autonomic computing adopted by IBM have the following four properties: [6]:

- **Self-Configuring:** The system adapts automatically to any dynamic changes in the environments.
- **Self-Healing**: Determines, diagnoses, and responds to disruptions.
- **Self-Optimizing** : Automatic observation and control of resources for the best performance regarding the defined demands;
- **Self-Protecting**: Anticipates, discovers, determines, and defends systems from any attack.

The complexity of systems management tasks increases whenever the distributed computing systems became more complicated. Where about 40% of computer problems occur because of errors done by the system administrators [7]. As a result, the approach of managing the system, which is depending on professional managers essentially, should be enhanced. To fix these issues when they appear, there is a need to use an efficient self-healing system. [8].

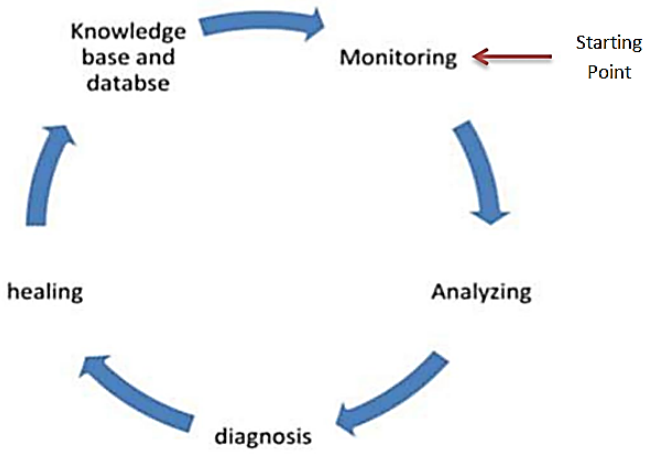

Figure (2) Circle of Self-management

3- The Vision of the Internet of Things

The goal of Internet of things “IoT” is to give the "smart" status to some functions of things, as well as the ability to connect and do complicated functions by themselves. The implementation can be encapsulated as services and the job carried out by composing the services.

It is worth noting that there are two advantages in IoT services which are monitoring and actuation. Monitoring is considered as continued executions, while actuation is done by triggering. The stream of input data is assembled into batches, where every batch is exposed to a series of computations, organized as a dataflow graph. The combination can be processing various batches in the same time. Moreover, some of them can be executing simultaneously.

Internet of things can be defined as a paradigm where the objects have sensors, processors and actuators. Moreover, they are connected with each other to do specific purposes. It can be considered as an interaction between the physical and digital world. Nowadays, the devices and applications can connect to the internet via sensors, actuators, processors, and transceivers.

Sensors and actuators are making any device interact with the physical world. In case of robots, the smart motors and

applications are considered as actuator. If the smart motor is connected to any device, it can be controlled by any browsers. The actuator is used to manipulate the physical world, like controlling the temperature in smart homes, where the actuator transforms the electrical signal input to an action. This kind of technology combines big data that can be useful in case of stored, categorized, and processed.

It can be said that IoT is not one type of technology, but a set of different technologies connected to each other. Real world objects will be uniquely identifiable and connected to the Internet Sprayer or extinguisher

4- The Vision of The artificial immune system

Thanks to natural defense system or (the immune system) in the human bodies, for surviving in this planet over millions of years. This system offers protection against the foreign molecules (called antigens), like fungi, bacteria, viruses and other parasites. The protection of human body that is achieved by this system through monitoring, studying and recognizing these foreign molecules which get in the human body. After that, the system makes a response against them via creating producing and releasing antibodies in order to attack the antigens and overcoming them from the body and release it from infections. In order to remove the threat, IS should be capable to distinguish between foreign molecules and the molecules/tissues which form itself to prevent auto-immune responses. The artificial immune system (AIS) includes a hopeful technique biological-based approaches that are applied to solve different problems in the network intrusion detection and security fields. The inspiration of AIS is from the human immune body, the human body has capability to differentiate inner cells and a group of atoms bonded together of the body from diseases, known as self and non-self, and protects the body.

The onset of the timeline of the immune response is when confronted with the initial pathogen (or initial vaccination) and manages to the establishment and maintenance of active immunological memory.

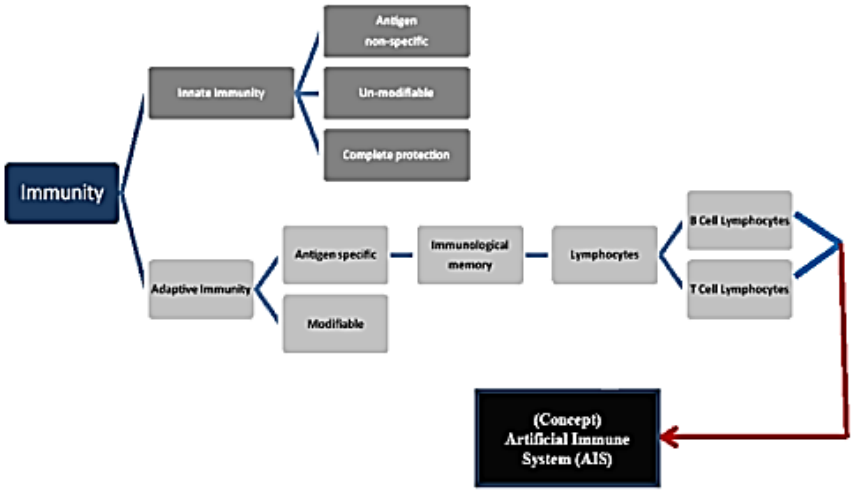

Figure (3) Human Immune System

The artificial immune system was introduced and motivated thru the natural immune system. Different application areas sometimes use several AIS such as clustering, web mining, classification, virus detection, image processing,

learning, robotic control, anomaly detection and bio-informatics and its common algorithms like clonal selection, negative selection … etc. [7].

After critically reviewing the literature, four primary AIS algorithms were reached for developing different AIS applications.

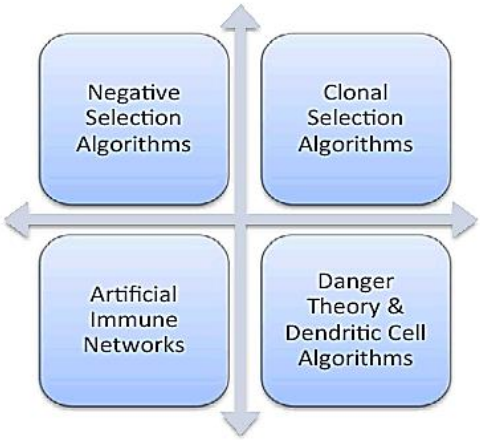

Figure (4) AIS Algorithm

5. Research Results

Through the study of the Internet of things and the human immune system, both systems need self-management; we suggest the use of immune system algorithms to achieve the goal of the Internet of things to access self - management as follows:

1. The self-management contains four functional domains and any system in the universe that contains these four functions (self-formation, self-healing, self-improvement, and self-protection). It is used or within the field of self-management.

2. Internet stuff is a phrase of a network of things working in isolation from humans, this already needs these functions and we will address them in detail:

i. Self-formation: Internet of things is also a network and any network you need Network configuration. It is a process of setting up the network, play and play controls to support enterprise networking and owner. This generic term includes multiple configurations on network devices, software, hardware, and other supporting components (specifying the correct IP addresses and path settings, default network settings, network name, and ID/password, to enable network connection)

ii. Self-healing: Internet of things deals with smart devices that have the ability to handle bugs that get this example SONET, Self-healing networks as one of the most advanced mechanisms used to achieve live SONET networks. Several plans have been proposed and studied because of the rapid progress in the development of high-IQ elements (NEs). A self-distribution network based on DCS from the point of view of its control algorithms. TRANS is a self-healing algorithm in details. It has eligible features like offering quick and flexible restoration with level and track level restoration on a singular STS-1 channel, and the capability to manage various failures and even a node.

iii. Self-development: This function should be available on the Internet of things system. For example, electronic health systems, sensors and system-related objects must have the ability to adapt and decide on the associated situation.

iv. Self-protection: Security is the necessary task of all systems network in general, especially when dealing with the network of sensors and management over the Internet and therefore requires the use of certain possibilities to prevent unauthorized people from penetrating the system, for example (use of an eye or programmed tags).

References

[1] F. Javed, M. T. Hassan, K. N. Junejo, N. Arshad, and A. Karim,"Self-Calibration: Enabling Self-Management in Autonomous Systems by Preserving Model Fidelity", IEEE 17th International Conference on Engineering of Complex Computer Systems, 2012.

[2] D. Naeem "Secure Chatting System with Self-Healing Service" dissertation, Computer Sciences of the University of Technology,2018.

[3] Andrew Watkins, Jon Timmis and Lois Boggess, "Artificial Immune Recognition System (SAIRS): An Immune-inspired Supervised Learning Algorithm," Genet. Program. Evolvable Mach., vol. 5, no. 3, pp. 291–317, Sep. 2004.

[4] Adnan Darwiche, "Modeling and Reasoning with Bayesian Network", Cambridge University Press, New York, USA, 2009.

[5] Ali A. Ghorbani et. al. "Network Intrusion Detection and Prevention Concepts and Techniques", Springer, New York, 2010.

[6] J. M. S. Vilchez, I. G. B. Yahia,and N. Crespi, " Self-healing Mechanisms for Software Defined Networks", HAL-archive ouverte , 2014

[7] A. M. Zeeshan,"Design and Evaluation of Self-Healing Solutions for Future Wireless Networks", the Faculty of Information Technology of the University of Jyväskylä , 2016.

[8] Nicholas Wong et.al., "Artificial Immune Systems for the Detection of Credit Card Fraud: An Architecture Prototype and Preliminary Results", Info. Systems, January 2012.

[9] R. Sridevi and Rajan Chattemvelli, "Genetic Algorithm and Artificial Immune System: A Combinational Approach for Network Intrusion Detection", IEEE-international Conference on Advances in Engineering Science and Management (ICAESM), March 30,31,2012.