A Framework for Constructing a New Model of Web Database Security

Eslam Mohsin Hassib
IT Engineer , ERG company, ElmahlahAlkobra, Egypt

Amany Mahmoud Sarhan
Associate Professor Computer and systems Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt.

Ahmed Ibrahim Saleh
Computer and systems Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt.

ABSTRACT

Through the last decade, web database security had become a very important issue when designing web database applications. Those applications usually include critical processes such as electronic-commerce web applications that include money transfer via visa or master cards. Security is a critical issue in other web based application such as sites for military weapons companies and national security of countries. The main contribution of this paper is to introduce a new web database security model that includes a combinationoftriplesystem ; (i) Host Identity protocol(HIP) in a new authentication method called DSUC (Data Security Unique Code), (ii) a strong filtering rules that detects intruders with high accuracy, and (iii) a real time monitoring system that employs the Uncertainty Degree Model (UDM) using fuzzy sets theory. It was shown that the combination of those three powerful security issues results in very strong security model. Accordingly, the proposed web database security model has the ability to detect and provide a real time prevention of intruder access with high precision. Experimental results have shown that the proposed model introduces satisfactory web database protection levels which reach in some cases to detect and prevent more that 93% of the intruders.

Keywords:intrusion detection, intrusion prevention, web database, security, HIP.

1.INTRODUCTION

Recently, due to the dramatic development of network technologies and the popularity of the Internet, web database security has become an appealing research area. It was reported by Computer Security Institute (CSI) and the FBI that; 70% of computer users reported that their networks were attacked over the last year [1]. Moreover, Denial of Serviceattacks increased 33%over the same period. The wonderful issue is that all of these took place across networks, where firewalls had been installed in 90 percent of instances. It is apparent that firewalls are not always effective against many intrusion attempts. Firewalls are also typically employed only at the network perimeter. However, many attacks are usually launched from within an organization[2]. For illustration, Virtual private networks (VPNs) provide access to the internal network that often bypasses the firewall. From another point of view, the wide evolution and Popularity of wireless networks have changed the way that organizations work as well as offering new availabilities; however, they also introduce new security threats. While an intruder needs a physical infrastructure to access a wired network in order to launch his attack, a wireless network allows anyone within its range to passively monitor the traffic or even start an attack[3].Itis clear that enterprises and government agencies need security vendors to step up and deliver innovative solutions that effectively protect their networks from malicious attacks and misuses[4].Today, the network is the business. Driven by business needs, enterprises and government agencies have developed sophisticated, complex information networks, incorporating technologies as diverse as distributed data storage systems, encryption techniques, Voice over IP (VoIP), remote and wireless access, and Web services[5]. These networks have become more permeable as business partners access services via extranets; customers interact with the network through e-commerce transactions or Customer Relationship Management (CRM) processes; and employees tap into company systems through Virtual Private Networks (VPN). So, it becomes necessary to insure that access to secure web-based databases is restricted to only the authorized users. Moreover, authorized users should not break their privileges. In the late 1990s, as hacker attacks, viruses, and network worms began to affect the internet services, intrusion detection systems were developed to identify and report attacks. Although, Intrusion Detection technologies may be effective at detecting suspicious activity, but do not provide protection against attacks. Existing Intrusion Detection Systems (IDS) can be divided into two types: (i) misuse detection, which contains a database that stores known intrusion techniques or behaviors and detects intrusions by comparing the current users' behaviors against the database; (ii) anomaly detection, which analyzes user behaviors, and checks if the system is being used in an unauthorized fashion [6].Intrusion Prevention Systems (IPS) is more advanced version of Intrusion Detection Systems that provides powerful protection by blocking intrusion attempts, protecting against malware, Trojans, DoS attacks, malicious code transmission, backdoor activity and blended threats. An IPS is any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful[7]. Basically an IPS is a firewall which can detect an anomaly in the regular routine of network traffic and then stop the possibly malicious activity. However, IPS also has several drawbacks such as; (i) it usually generates false positives that can create serious problems if automated responses areused, (ii) it may cause network bottlenecks, and (iii) it is expensive as it is still a new technology. Also, in spite of its ability to prevent attacks on real time, Intrusion prevention systems (IPSs) do not introduce a satisfactory web database protection level. Hence, new techniques need to be investigated.The rapid growth of the Internet increases the importance of connecting to existing databases. The Web, with all its versatility, is putting database

security as a key issue. Access to web-enabled databases containing sensitive information must be made available only to authorized users. Also, a crucial problem in nowadays websites is that; web servers cannot handle large amounts of faking requests, which in turn overloads the web database server[8]. To go around such hurdle, web database access must be carefully controlled using a strong Filter. Finally, with the increased use of mobility devices, techniques that require the validity of a host and/or a user discarding the change in IP address is strongly required. Another ill news is that; the most attacks are usually made by "authorized" users of the system. To the best of our knowledge, implementing an efficient web database security model has not been addressed yet. Accordingly, web database security is still more complex than the proposed solutions.Many hurdles stand in the way of achieving the maximum protection of web databases. Accordingly, this issue is still an elusive problem that attracts the interests of many researchers [9].The focus of this paper is to shed some light on how databases can be used in a secure manner when connecting to the World Wide Web. To accomplish such aim, the paper introduces a novel web database security model that including a new authentication method called DSUC (Data Security Unique Code) which is a hardware component like USB flash memory contain a unique MAC code like LAN adapter ,this MAC address must be attached to the user host to pass the security check by using HIP(Host Identity protocol) with a strong filtering server and finally a real time monitoring system by using fuzzy set theory called UDM (Uncertainty degree model) for monitoring users operations in real time.

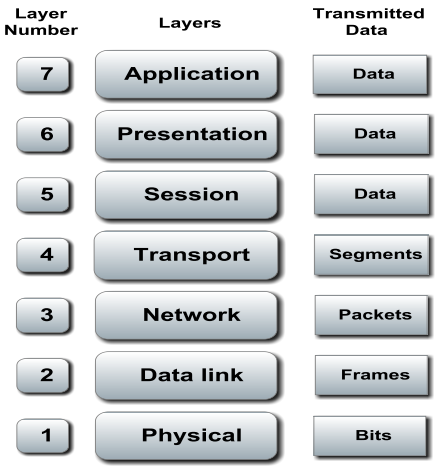


Figure (1):ISO/OSI network model layers.

In spite of the dual role of IP addresses previously mentioned, it is becoming problematic for several reasons. A huge number of attempts to solve these problems have led to the development of the Host Identity Protocol (HIP). HIP introduces a newnamespace composed of Host Identities (HIs). A Host Identity is a cryptographic entity which corresponds to an asymmetric key-pair. The public identifier associated to a HI is consequently the public key of the key-pair[12]. The new identity domainintroduced by HIP enables the separation of the roles of IP addresses. While IP addresses keep their locator role in the network layer, HIs will assume the identifier role in upper layers [13]. Therefore, considering the ISO/OSI Network model, the HIP protocol introduces a new layer between the network and transport layers as depicted in Figure (2).

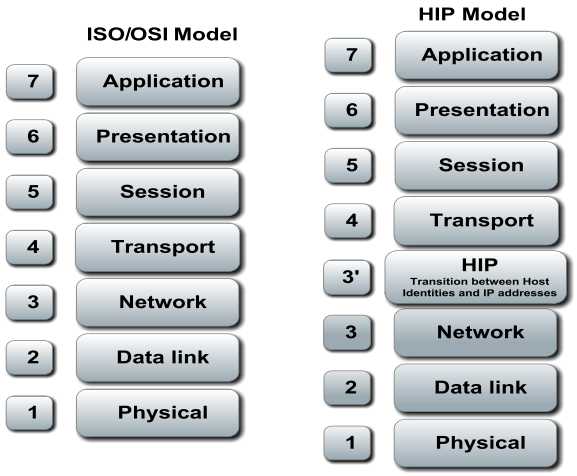
2.BACKGROUND AND BASIC CONCEPTS:

In this section, a simple view for the Host Identity Protocol (HIP) is illustrated. Then, Fuzzy logic is explained in details.

2.1. Host Identity Protocol:

Currently, communications through computer networks are usually described with the ISO/OSI reference model, which contains seven layers illustrated in Figure 1. In such model, each layer; (i) uses functions from lower layers, (ii) provides new functionalities to upper layers, and (iii) has its own protocols to communicate with its peers located at the other network computers. The network and transport layers, as illustrated in figure 1, play an important role in Internet communications. Network layer is usually managed by the Internet Protocol (IP), while the transport layer is included to handle the data segments transmitted in IP packets. Common protocols for the transport layer are; (i) Transmission Control Protocol (TCP), or (ii) User Datagram Protocol (UDP)[10].

Internet protocol defines one of the two main namespaces currently used in the Internet, the namespace composed of IP addresses. The second main namespace is composed of Domain Name System (DNS) names[11]. While DNS names are used as identifiers on application level, IP addresses are most important and are used in the ISO/OSI network model from the network layer to the application layer.



Figure(2):Common ISO/OSI network model layers and HIP network model layers.

In the HIP layer and in upper layers, Host Identifiers replace IP addresses. The conversion between a Host Identity and the corresponding IP address is established in the HIP layer[14]. To allow legacy applications to easily use HIs instead of IP addresses, HIP defines two types of identifiers that are numerical values of the same length as common IPv4 or IPv6 addresses. The main identifiers are 128-bit Host Identity Tags (HITs) and a limited version of them is 32-bit Local Scope Identifiers (LSIs).The introduction of a new namespace and the use of the new HIP protocol imply a new way to establish communications between two hosts. HIP communications are divided in two main phases: the HIP Base Exchange and the secured data transfer[15]. The HIP Base Exchange uses specific HIP packets to establish a connection between two end hosts, represented by their Host Identities. The resulting communication is therefore based on a pair of HITs or LSIs. The Base Exchange also allows the exchange and negotiation of parameters and cryptographic keys for the communication. After the Base Exchange is completed, the end-hosts can establish

secured communications, based on HIs, and exchange data in a secured way. The data transfer relies on an existing end-to-end security protocol, which is typically but not necessarily the IPsec ESP protocol[16].

Accordingly, the HIP Operation sequence can be expressed in the following steps, which are also illustrated in figure (3); (i) the Responder must register its Host Identity, and registered its domain namespace in the DNS Server in advance, (ii) the Initiator must register its Host Identity, and registered its domain namespace in the DNS Server in advance, (iii) the client (Initiator) sends packet I1 to the RVS starting the HIP authentication. After validating it, the RVS forwards I1 to the Responder (in the Web server). (iv) After checking the packet I1, if I1 has a (UI&HI(binding flag added by RVS, the Responder (in the Web server) directly sends packet R1 to the Initiator, The R1 contains a challenge puzzle to HI and UI, that is, a cryptographic challenge that the Initiator must solve before continuing the exchange.
In addition, it contains the initial Diffie-Hellman parameters and a signature. (v)In the packet I2, the Initiator (client) must display the solution to the received challenge puzzle .Without a correct solution, the Responder (in the Web server) discards the I2 message. The I2 also contains a Diffie-Hellman parameter that carries needed information for the Responder. (vi)The packet R2 finalizes the 4-way handshake, containing the SPI (Security Parameters Index) value of the Responder[17].

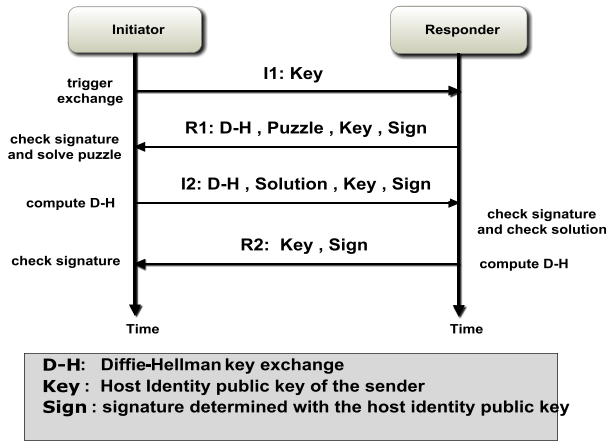


Figure (3): HIPBase Exchange operations sequence.

2.2. Fuzzy :

The fuzzy logic was specifically designed to mathematically represent uncertainty. However, the story of fuzzy logic started much more earlier . . . To devise a brief theory of logic, and later mathematics, *Aristotle* posited the so-called"Laws of Thought"[18]. One of these, the"Law of the Excluded Middle," states that every proposition must either be *True* (**T**) or *False* (**F**). Even when *Parmenides* proposed the first version of this law (around 400 Before Christ) there were strong and immediate objections: for example, *Heraclitus* proposed that things could be simultaneously *True*and*not True*.
It should be noted that *Knuth* also proposed a three valued logic similar to Lukasiewicz's, from which he predicted that mathematics would become even more fashionable than in traditional bi-valued logic. The notion of an infinite-valued logic was introduced in Zadeh's seminal work "Fuzzy Sets" where he described the mathematics of fuzzy set theory, and by extension fuzzy logic[19]. This theory proposed making the membership function (or the values **F** and **T**) operate over the range of real numbers [0, 1]. New operations for the calculus of logic were proposed, and showed to be in principle at least a generalization of classic logic. Fuzzy logic provides an inference morphology that enables approximate human reasoning capabilities to be applied to knowledge-based systems. The theory of fuzzy logic provides a mathematical strength to capture the uncertainties associated with human cognitive processes, such as thinking and reasoning[20]. The conventional approaches to knowledge representation lack the means for representing the meaning of fuzzy concepts.
For example, uses a fuzzy Adaptive Resonance Theory (ART) and neural network to detect anomaly intrusion of database operations, by monitoring the connection activities to a database. As a result, we have a motivation of integrating fuzzy set theory and intrusion detection technique to deal with *Hidden Anomaly* in databases precisely in real time. The advantage of using fuzzy logic because it can be used to calculate the intermediate numbers like a probability between (0-1).In our research that's a very important point because we want to calculate the uncertainty degree which is a fraction of integer 1.We will use a fuzzy membership function called (triangular fuzzy number) to achieve this goal and that what we will illustrate in the next sections[21].

2.3. Denial of service attacks (DOS):

A DoS attack is a malicious attempt by a single person or a group of people to disrupt an online service. DoS attacks can be launched against both services, e.g., a web server, and networks, e.g., the network connection to a server. The impact of DoS attacks can vary from minor inconvenience to users of a website, to serious financial losses for companies that rely on their on-line availability to do business. On February 9, 2000, Yahoo, eBay, Amazon.com, Buy.com, the FBI, and several other Web sites fell victim to DoS attacks resulting in substantial damage and inconvenience [22]. As emergency and essential services become reliant on the Internet as part of their communication infrastructure, the consequences of DoS attacks could even become life-threatening. Hence, it is crucial to deter, or otherwise minimize, the damage caused by DoS attacks.

2.3.1 Technical Problems:

There are four different ways to defend against DoS attacks: (1) attack prevention; (2) attack detection; (3) attack source identification; and (4) attack reaction.
Attack preventionaims to fix security holes, such as insecure protocols, weak authentication schemes and vulnerable computer systems, which can be used as stepping stones to launch a DoS attack. This approach aims to improve the global security level and is the best solution to DoS attacks in theory. However, the disadvantage is that it needs global cooperation to ensure its effectiveness, which is extremely difficult in reality. Hence, the challenge is how to develop a scalable mechanism with low implementation cost[23].

Attack detection aims to detect DoS attacks in the process of an attack. Attack detection is an important procedure to direct any further action. The challenge is how to detect every attack quickly without misclassifying any legitimate traffic.

Attack source identification aims to locate the attack sources regardless of the spoofed source IP addresses. It is a crucial step to minimize the attack damage and provide deterrence to potential attackers. The challenge for attack source identification is how to locate attack sources quickly and accurately without changing current Internet infrastructure.

Attack reaction aims to eliminate or curtail the effects of an attack. It is the final step in defending against DoS attacks, and therefore determines the overall performance of the defense mechanism. The challenge for attack reaction is how to filter the attack traffic without disturbing legitimate traffic.

2.4. Previous Efforts:

Early in the research into such systems two major principles known as anomaly detection and signature detection were arrived at, the former relying on flagging all behavior that is abnormal for an entity, the latter flagging behavior that is close to some previously defined pattern signature of a known intrusion. The problems with the first approach rest in the fact that it does not necessarily detect undesirable behavior, and that the false alarm rates can be high. The problems with the latter approach include its reliance on a well-defined security policy, which may be absent, and its inability to detect intrusions that have not yet been made known to the intrusion detection system. It should be noted that to try to bring more stringency to these terms, we use them in a slightly different fashion than previous researchers in the field[24]. An intrusion detection system consists of an audit data collection agent that collects information about the system being observed. This data is then either stored or processed directly by the detector proper, the output of which is presented to the SSO (System Security Observer), who then can take further action, normally beginning with further investigation into the causes of the alarm. Most, if not all, would agree that the central part of an intrusion detection system is the detector Proper and its underlying principle of operation. Obviously, the source of our troubles is an action or activity that is generated by the intruder. This action can be one of a bewildering range, and it seems natural to start our research into how to construct a detector by first studying the nature of the signal that we wish to detect. From the nature of the source we move to the question of how to observe this source, and what problems we are likely to have in doing so. In a security context, we would probably perform some sort of security audit, resulting in a security audit log. Sources of frustration when undertaking logging include the fact that we may not be able to observe our subject directly in isolation; background traffic will also be present in our log, and this will most likely come from benign usage of the system. In other words, we would have an amount of traffic that is to varying degrees similar to the subject we wish to observe. However, we have found no study that goes into detail on the subject of what normal traffic one might expect under what circumstances. With a sufficiently narrow assumption of operational parameters for the system, we believe useful results can be achieved [25]. This brings us to the results of the security logging—in other words what can we observe—and what we suspect we should observe given an idea of the nature of the security violation, background behavior, and observation mechanism. One issue, for example, is being precisely what data to commit to our security log. How then to formulate the rule that governs our intrusion detection decision? Perhaps unsurprisingly given the state of research into the previous issues, this also has not been thoroughly addressed. More often than not we have to reverse engineer the decision rule from the way in which the detector is designed, and often it is the mechanism that is used to implement the detector rather than the detection principle itself. For that reasons we have to do the best we can to classify as precisely as possible given the principle of operation of the detector. Some work is clearer in this respect, In the light of this; the main motivation for taking an in-depth approach to the different kinds of detectors that have been employed is that it is natural to assume that different intrusion detection principles will behave differently under different circumstances [26].

3. TheProposed Hybrid Intrusion PrevisionSystem (HIPS):

The general structure of the proposed HIPS is illustrated in figure (4). It consists of several modules that will be discussed with the system sequential operations in more details in the following subsections.

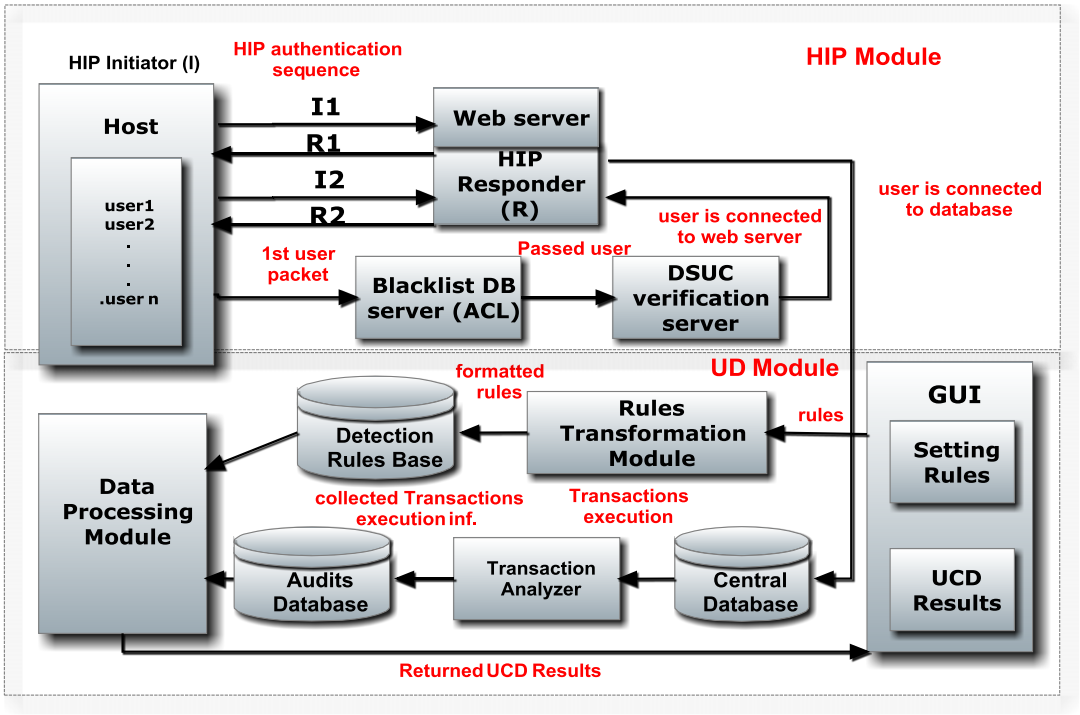


Figure (4): Architecture of Proposed Model.

Figure (4) depicts the architecture of the proposed Model which consists of the following modules:

1. ***The user host*** which contains any number of hosts for accessing the web server database over the internet which represents the HIP Initiator in the client side in Host Identity Protocol authentication method.
2. ***The blacklist database server;*** which plays the role of access control list server containing a real time updated database consists of the IP addresses and MAC addresses of the blocked hackers.
3. ***Data Security Unique Code (DSUC) server;*** which authenticates the user identity (user name and password) and host identity (the flash memory).
4. ***The web server***; which contains the requested Database and represents the HIP Responder in Host Identity Protocol authentication method.
5. ***The graphical users interface (GUI)***; that represents the connection between the web server administrator and the system, which includes Setting Rules and display uncertainty-degree Results. Setting Rules allows users to set up monitoring steps. These monitoring steps are then formatted and stored into Detection Rules Base as Rules. The information about each database transaction execution is stored into Audits Base by Sensor (Transaction analyzer). Event Analyzing selects every new audit record from audits Base, and then checks against the detection rules in Detection Rules Base**:** Finally, Event Analyzing calculates uncertainty degree for the audit record, and sends the results to uncertainty degree Result.
6. ***Audits Base;*** which is built to store the monitoring records generated by Sensor, while Detection Rules Base is used to store detection rules.
7. ***Setting Rules;*** which used to define detection rules, specifies which attributes of transactions to monitor, what types of membership functions to use, etc.
8. ***Rules Transformation Module;*** When the information of the monitoring attributes and membership function has been chosen, Mapping to Rules translates it into the format of detection rules to store in Detection Rules Base.
9. ***Transaction Analyzer;*** which monitors the transactions of databases in real time. By analyzing each transaction execution, and collects information about the transaction execution, and then stores it in Audits Base.
10. ***Data Analyzing Module;*** for each record in Audits Data Base, Event Analyzing Module is processed and matched against the rules in Rules Data Base. The value of the monitored attribute is then obtained. By substituting this value in the membership function defined in the rule, the result of the function is calculated as the degree of dubiety.

3.1.Host Identity Protocol (HIP):

As illustrated in Figure (4), the HIP Responder is in the Web server while the clients (host and user) accessing the web database represent the HIPInitiator. The HIP authenticating method is located in the Web server of database system. Also, The BS (blacklist server) cooperates with the Web server to authenticate both the User Identity and Host Identity.

What is Data security Unique code(DSUC)?

We have considered the host identity in a DSUC (Data Security Unique Code) which is a hardware component like flash memory that contains specific code for each user thatthe user must have it attached to his host to pass the security check in order to be able to access the database. So, if there is a user in Egypt wants to access the company database in Syria so, he must have his own DSUC attached in the pc that he want to use it to access the database in France and provide a true user name and true password along with true DSUC.

3.1.1: HIP Packet structure:

Next Header	*Header Length*	*Packet Type*	*Version*
Checksum		*Controls*	
Sender's Host Identity Tag(HIT) (User's DSUC)			
receiver's Host Identity Tag(HIT) (Web Server DB Identifier)			
HIP Parameters			

Figure (5):HIP Packet structure

The HIP packet structure is the same as HIP packet structure as illustrated in figure (5) consists of the following fields:

The HIP header is logically an IPv6 extension header. The Header Length field contains the length of the HIP Header and HIP parameters. The HIP Version field contains the used version, currently 1. The Checksum field is an ordinary checksum for the whole message. The Controls field conveys information about the structure of the packet and capabilities of the host. A sending host can set the HIP message exchange to anonymous; the receiving host of an anonymous HI may choose to refuse it. Where the sender's HIT represent the DSUC of each user and the receiver's HIT represent the company web DB code. The HIP Parameters field contains the various HIP options and extensions.

3.2.Filtering System (Blacklist database):

The main objective of this server is to protect the web server from Denial of Service Attacks (DOS). It's a server that contain (black list) of banned usersIPs and MAC addresses, I the user has entered wrong login data, the system will give the user five attempts to enter the correct login data then his IP and Mac addresses will be added to the blacklist database and he will be blocked from accessing the web server for the next 24 hours.

3.3.Uncertainity degree model(UDM):

Given a vector of a random variable *X* and *n* observations *X*1,…,*Xn*, the goal of the statisticalsub-model of *X* is to determine whether a newobservation*Xn*+1is abnormal with respect to theprevious observations. The mean *avg*and the standarddeviation*stdev*of 1*X*,…,*Xn*are defined as shownin Eq. (1) and Eq. (2):

$$avg = \frac{X_1 + X_2 + .. + X_n}{n} \qquad (1)$$

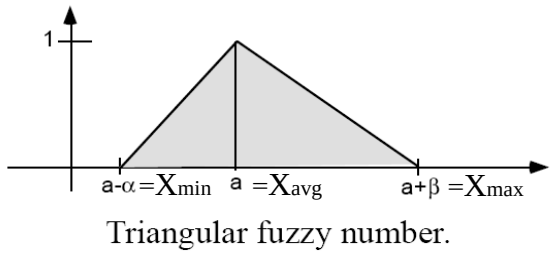
$$stdev = \sqrt{\sum_{i=1}^{n} (X_i - avg)^2} \qquad (2)$$

A new observation *Xn +1*is defined to be abnormal if it falls outside a *confidence interval* that is standard deviations from the mean, which is denoted by *CI as shown in Eq.(3)*:

$$CI = avg \pm dev \qquad (3)$$

Where*dev= d × stdev*with*d* as a parameter. Therefore, it would apply for the case of *Hidden Anomaly*. Membership functions are used to "measure" the *uncertainty* degrees for each transaction. For each transaction, a value of variable *X* can be observed. It can be mapped into the interval [*0,1*] by a membership function. We define 0 means *completely acceptable*, and 1 implies anomaly or *completely unacceptable*. The values between 0 and 1 are called *uncertainty degree*. In this way, the dubiety of transactions can be denoted in a unified form. We will use (triangular fuzzy membership function) as illustrated in figure (6) which is defined as A fuzzy set A is called triangular fuzzy number with peak (or center) a, left width $\alpha > 0$ and right width $\beta > 0$ if its membership function has the following form as shown in Eq. (4):

$$f(x) = \begin{cases} (a-x)/\alpha & if \quad a-\alpha \le x \le a \\ (x-a)/\beta & if \quad a \le x \le a+\beta \\ 1 & otherwise \end{cases} \qquad (4)$$



Triangular fuzzy number.

Figure (6): Triangular Fuzzy membership function.

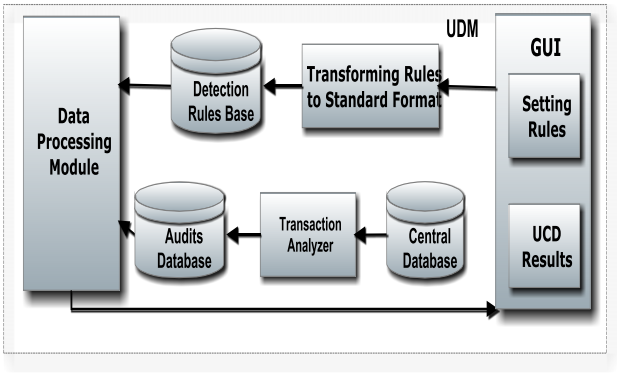


Figure (7): Architecture of the Uncertainty Degree model.

Figure (7) depicts the architecture of transaction monitoring for database based on UDM which consists of the following modules;

1. The graphical users interface (GUI) that represents the connection between the web server administrator and the system, which includes Setting Rulesand display uncertainty-degree Results. Setting Rulesallows users to set up monitoring steps.These monitoring steps are then formatted and stored into Detection Rules Base as Rules. The information about each database transaction execution is stored into AuditsBase by Sensor (Transaction analyzer). Event Analyzing selects every new audit record from audits Base, and then checks against the detection rules in Detection Rules Base**:** Finally, Event Analyzing calculates uncertainty degree for the audit record, and sends the results to uncertainty degree Result.
2. Audits Base, which is built to store the monitoring records generated by Sensor, while Detection Rules Base is used to store detection rules.
3. Setting Rules, which used to define detection rules, specifies which attributes of transactions to monitor, what types of membership functions to use, etc.
4. Transforming to Rules: When the information of the monitoring attributes and membership function has been chosen, Mapping to Rules translates it into the format of detection rules to store in Detection Rules Base.
5. Transaction Analyzer which monitors the transactions ofdatabases in real time. By analyzing each transaction execution, and collects information about the transaction execution, and then stores it in Audits Base.
6. Event Analyzing; for each record in Audits Base, Event Analyzing Module is processed and matched against the rules in Rules Base. The value of the monitored attribute is then obtained. By substituting this value in the membership function defined in therule, theresult of the function is calculated as the degree of dubiety.

3.4.System operation:

Figure(8) illustrates the sequential operations of the proposed HIPS which consist of three different phases, namely(i) initial filtering, (ii) authentication, and (iii) real time monitoring.

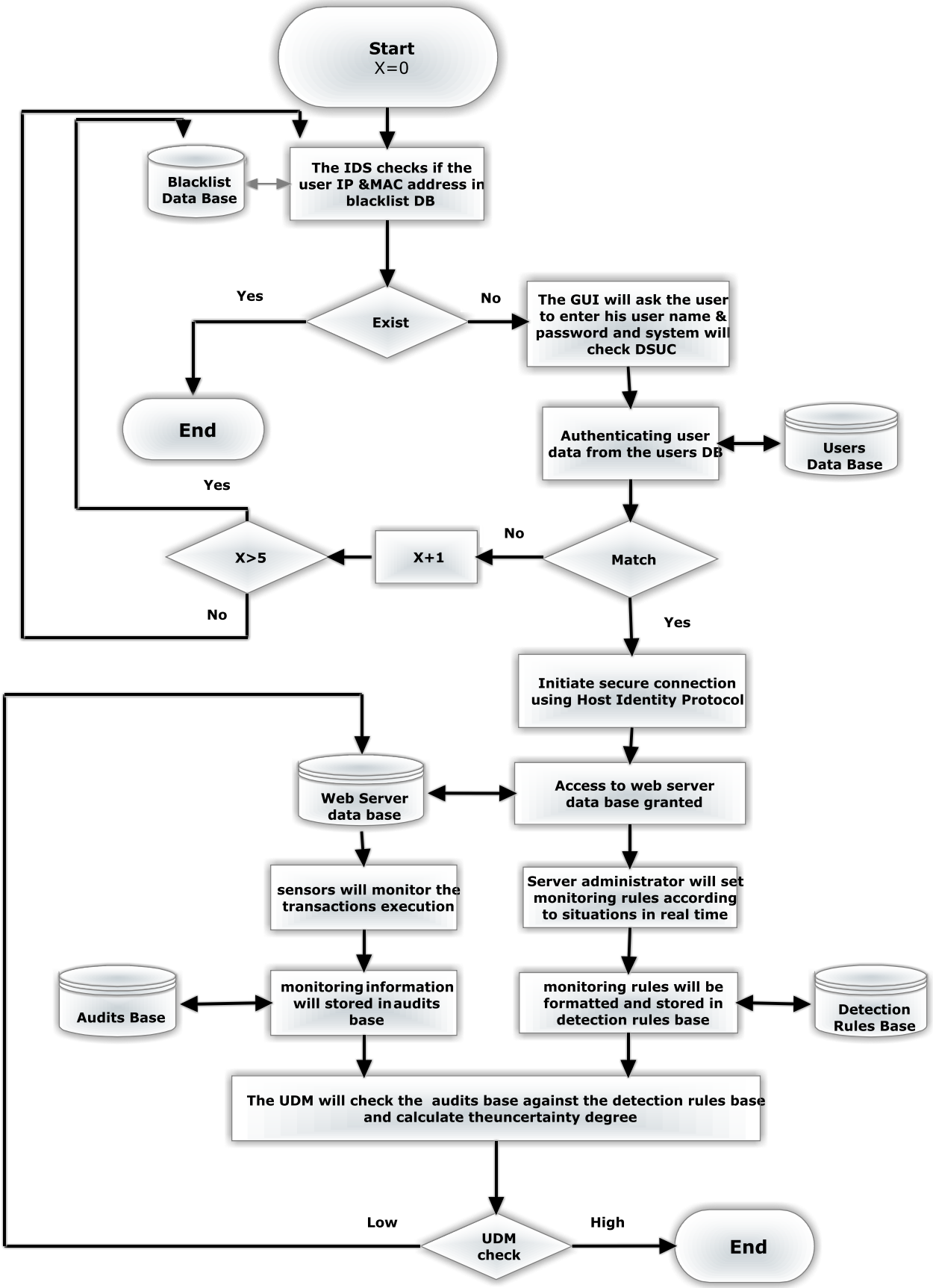


Figure (8): Flow chart of system operation sequence.

Phase 1: Filtering System check:

- When a new user activate the system the system will automatically get his IP address and MAC addresses from the network hash table and checks them in the blacklist DB if his IP address or MAC address exist the system will cancel his request silently.

Phase 2: Host Identity Protocol check:

- The system will ask the user to enter his login data(user name & password) then the system will check for the DSUC and checks them in the users database if there is any change in the three fields (user name, password, DSUC) the system will give him five attempts to enter the correct data then he will be blocked from accessing the system and his IP and Mac addresses will be added to the blacklist database.
- The blacklist database is cleared every 24 hours.
- If the entered data is correct, then the system will start the HIP Base Exchange operations sequence to initiate a secure connection to the web server database using Host Identity Protocol.
  Now, user will be allowed to enter the web server database and gets the desired data under certain constrains

Phase 3: Uncertainty Degree Model check:

- Now the system will work in two phases in real time, the monitoring rules had been set and stored in detection rules base, but if necessary the system administrator will set new monitoring rules and attributes to each user according to current situation, and the system will monitor the transactions execution by transaction analyzer and store the monitoring information in the Audits base.
- The system will uses the fuzzy membership function as shown in Eq. (4) to calculate the degree of uncertainty:

$$f(x) = \begin{cases} (a-x)/_{\alpha} & if \quad a-\alpha \le x \le a \\ (x-a)/_{\beta} & if \quad a \le x \le a+\beta \\ 1 & otherwise \end{cases} \quad (4)$$

- If the Uncertainty degree is high (close to 1) the system will automatically knock out the user and block him from accessing the web server database in future.

4.EXPERIMENTAL RESULTS:

Initially, we need to define two terms in our system, which are (i) Analyzer Record, and (ii) Detection Rule. Analyzer Record is used for recording the information about each database operation. This data structure is 6-tuple recording information of each database transaction: <An, Un, SQLText, Time, Data1, Data2> as illustrated in table (1). To make it clearer, from now on in this paper, we will use the term *Analyzer Record* instead of *transaction*.

Table (1): Analyzer Record structure.

Term	Meaning
An	Is the identifier for each Analyzer Record.
Un	records the user name of the transaction
SQLTEXT	Records the content of the SQL statement of the transaction.
Data1	Is the first data field that the transaction relates to, for example; the data value before update.
Data2	Is the second data field that the transaction relates to,forexample; the data value after an update.
Time	Specifies a number of hours as a time range. The audit records occurred in that time range before the currently being tested will be seen by the rule.

On the other hand, the Detection Rule is the namespace for specifying the format of the detection rules. This data structure is 9-tuple defining the format of the detection rules: <Rn, Un, Action, Obj1, Obj2, Condition, Time, Function, Enable>, as illustrated in table (2).

Table (2): Detection Rulestructure.

Term	Meaning
Rn	starting with the letter *R* is the identifier for each detection rule.
Un	indicates which user the rule is aimed at.
Action	indicates what type of operations the rule is related to, such as *select, update, delete* and so on.
Obj1	is the first object that *Action* refers to, such as a table, a view or a procedure.
Obj2	is the second one. If *Obj1* is a table or a view, *Obj2* will be a field name.
Time	specifies a number of hours as a time range. The audit records occurred in that time range before the currently being tested will be seen by the rule.
Condition	indicates the condition of *Action*. Usually it is the condition part (*where* clause) of the SQL statement.
Function	is sub-tuple recording the information of the membership function used by the rule <***α***, **a**, ***B***> Where ***α***, **a**, and ***B***store the values of *a*, *b*, and *c* respectively (definition of membership function).

4.1.System Model:

Our experiments are performed on the DBMS of Microsoft SQL Server 2000 and Visual Basic.net 2003 on Microsoft Windows Xp, we will focus mainly in our tests on anomaly to show whether UDM can discover *Cumulated Anomaly* behaviors. The example database of SQL Server used in this study is a huge company for importing and exporting the electronic components that have a wide no. of branches all over the world. The table *Products* stores product data, including *PID (product ID)* and *UnitPrice*. Suppose there is a product whose*ProductID*is (100,130,160). In*Products*. Assume users, *Eslam, Adel, Ahmed,* are authorized to modify *UnitPrice*of*Products* .However, if the *UnitPrice*has been changed too much or too often, it could be suspicious. It is defined that *UnitPrice*should not be changed for more than 10 times in 30 days, and the sum of changed value should not be more than 5 Euro in 30 days. *Audits Base* and *Detection Rules Base* are built according to the two basic structures defined. *Data*. 15000 normal analyzer records are stored in the database. Our schema will include Time_stamps (system clock) in a period of one month. The values of fields SQLText are normal database operations in the form of SQL statements, including selecting data from a table, updating the data in a table, inserting data into or deleting data from a table, executing a procedure, and opening a database. Referring to the above assumptions, 3 additional audit records for *authorized users* updating *UnitPrice*of*Products are* constructed and mixed into the existing 15000 audit records. These 3 records are distributed into the range of one month. The *Detection Rules Base* contains three typical detection rules listed in the following table (in which the column of Enable is not listed to make the table not too wide). For example, R1 is used to monitor the audit records with *eslam*as Un, *update[Products] set UnitPrice=p where ProductID=100* as SQLText (where *p* is a number). The data items before and after update operation are recorded in the fields Data1 and Data2. When an audit record *R* which meets the demand of R2 occurs, the algorithm seeks the audit records meeting the demand of R2 which have occurred 720 hours before *R*, and sums up the margins between each pair of Data1

and Data2 in each of them. Then, the summation is substituted into *Fx* defined in R2. Finally, a result value of the function is calculated as the dubiety degree of that audit record. As this is a real-time process; an audit record will be examined as soon as it arrives.

4.2.The Experiment Detection Rules Table:

As illustrated in table (3), it is noted that each user has one rule. Hence, one test could be applied for each user (one test per rule). Also, The column time shows the period that the rule will be valid in hours, for illustration, R1 has time 480 hours to convert it into days (480/24=20 days).

Table (3): User's Detection RulesTable.

Rn	Un	ACTION	Obj 1	Obj 2	CONDITION	TIME_WINDOW	α	A	B
R 1	Eslam	Update	Products	UnitPrice	Product ID=100	480	52	54.5	57
R 2						720	52	55	58
R 3	Adel				Product ID=130	1440	51	53.5	56
R 4						720	51	53	55

4.3.Different users tests:

In the following subsections, the different tests for each user using rules illustrated in table 3 will be introduced in more details.

User No.1:

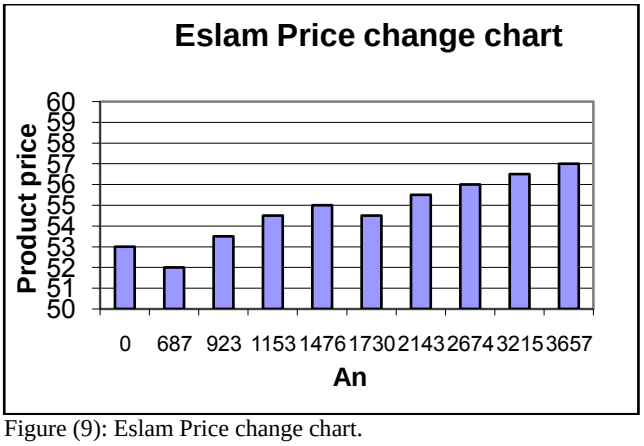


Figure (9): Eslam Price change chart.

Figure (9) shows us the audit record of operations for a user whose name is Eslam in 30 days. As we can see from the above figure that the summation of all changes are (58-52=6) > the max no. of changes allowed (5), so he did break the rule.

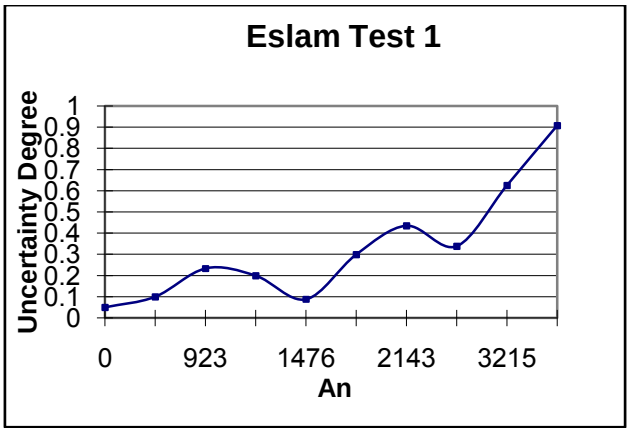


Figure (10): EslamUncertainty Degree chart.

The test applied with rules R1, we can see as illustrated inFigure (10)that the user behavior causes anomaly because he did break the rule of 5 euro change, and he made a change of 6 Euro. So, we can notice that the curve has reached the max value(1) which means completely Unacceptable. So, we can see that Eslam behavior causes anomaly.

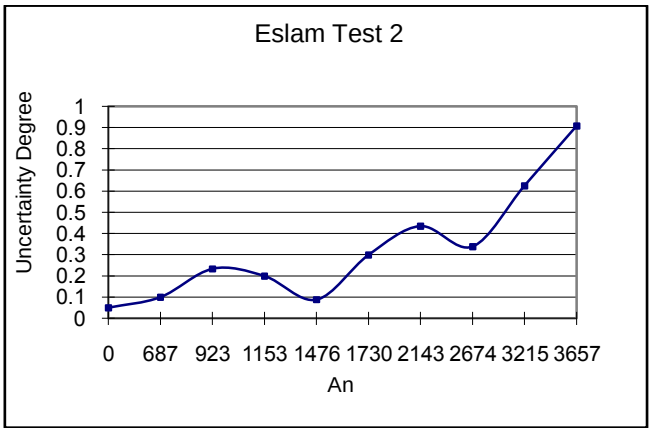


Figure (11): Eslam Uncertainty Degree chart.

Test2 applied with rules R1,R2,we can see from figure (11) that the user behavior cause anomaly because he did break the rule of 5 euro change ,and he made a change of 6 and 7 Euro.and we can see the Uncertainty degree increases gradually with no. of rules increases ,and we can see that Eslam behavior causes anomaly.

User No.2:

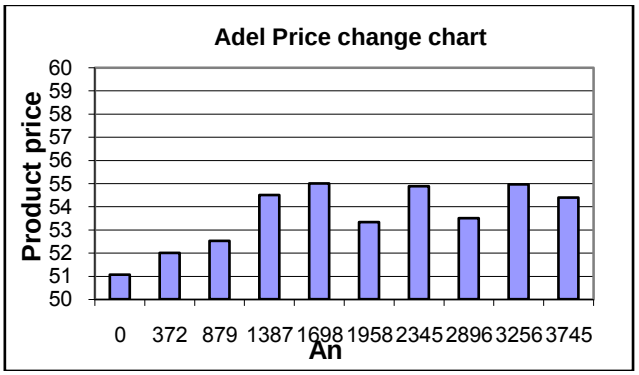


Figure (12): Adel Price change chart.

Figure (12)shows us the audit record of operations for a user whose name is Adel in 30 days. As we can see as illustrated

inFigure (12)that the summation of all changes are (55-51=4) <= the max no. of changes allowed (5), so he didn't break the rule.

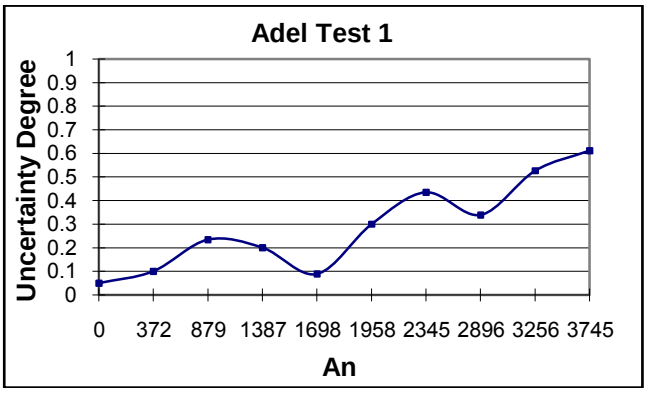


Figure (13): AdelUncertainty Degree chart.

The test applied with rules R3. we can see as illustrated inFigure (13) that the user behavior doesn't cause anomaly because he made a change of 4 Euro .So ,he didn't break the rule of 5 Euro change so, we can notice that the curve reach the value(.6) which means acceptable. So, we can see that Adel behavior doesn't cause anomaly.

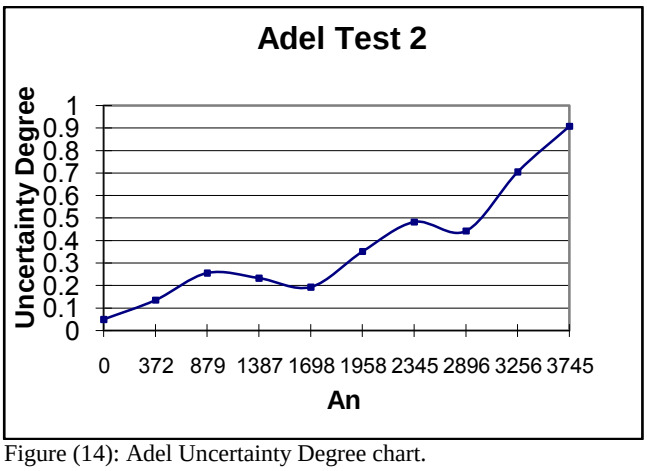


Figure (14): Adel Uncertainty Degree chart.

Test2 applied with rules R3,R4. we can see from figure (14) that the user behavior didn't cause anomaly because he didn't break the rule of 5 Euro change. and we can see that the Uncertainty degree increases gradually with no. of rules increases ,and we can see that Adel behavior doesn't cause anomaly.

5. CONCLUSION

In this paper, we have designed a new web database security model using ultra hybrid approach. Our model consists of three layers of security using DoS attack blocking server and DSUC (Data Security Unique code) and Uncertainty degree model. In this paper also, we have designed a simulator using VB.NET that simulates client server model for testing our model, the simulator is tested using many users and the results shows that our model is efficient and capable for blocking intruders from hacking into our system and discover suspicious behaviors of internal and authorized system users.

6.REFERENCES

[1] Michael C. Boeckeler, "Overview of Security Issues Facing Computer Users", GIAC Security Essentials Certification (GSEC), March 17, 2004.

[2] McAfee, "IntruShield Virtualization Delivering Real Benefits ", February 2005.

[3] Jack TIMOFTE, "Wireless Intrusion Prevention Systems", Revista*InformaticaEconomică*nr.3(47)/2008.

[4] Dr. FengminGong ," Next Generation Intrusion Detection Systems (IDS)", March 2002.

[5] B. Meyer, *Object Oriented Software Construction*, Prentice Hall, Upper Saddle River, NJ, USA, 2nd edition, 2005.

[6] Karen Scarfone, peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", (February 2007).

[7]ctcert,"Malicious software (Malware):A security Threat to the Internet Economy", OECD Ministerial Meeting on the Future of Internet Economy, Korea ,June 2008.

[8] Peter Stephenson , " investigatingComputer-related Crime A handbook for Corporate investigators ", 2000 by CRC Press.

[9] Ramesh Subramanian," Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions",Quinnipiac University, USA, 2008 by IGI Global.

[10] Damon Reed, "Applying the OSI Seven Layer Network Model To Information Security", November 21, 2003.

[11] R. Moskowitz, "Host Identity Protocol Architecture."RFC 4423 (Proposed Standard), may 2006.

[12] T. Okagawa et al., "Ip packet routing mechanism based on mobility management in aipbasednetwork," 14th International Conference on IntelligenceinNGN, 2009.

[13] PedryczWitold, Gomide Fernando. "An Introduction to Fuzzy Sets: Analysis and Design", 2008.

[14] P. Nikander, Host Identity Protocol (HIP) Domain NameSystem(DNS)Extensions, 2006.09.

[15] A. Matos, J. Santos, J. Girao, M. Liebsch, andR. Aguiar, "Host Identity Protocol Location PrivacyExtensions." Internet Draft (Work in Progress),March 2009.

[16] P. Nikander, "End-Host Mobility and Multi-Homing with Host Identity Protocol", 2006.06.

[17] Madson, C. and R. Glenn, "The Use of HMAC-SHA -1-96 within ESP and AH", RFC 2404, 2008

[18] S. Kent, "IP Encapsulating Security Payload (ESP)", (RFC 4303), 2005.12.

[19] Sin Yeung Lee, WaiLup Low, Pei Yuen Wong. Learning fingerprints for a database intrusion detection system. ESORICS 2002.

[20] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach," *Transactions on SoftwareEngineering*, 2005.

[21] Chung C Y,Gertz M, Levitt K. DEMIDS: A Misuse Detection System for Database Systems. In:The Third Annual IFIP 11.5 Working Conf. on Integrity and Internal Control in Information Systems, 2009

[22] L. Garber. \Denial-of-service attacks rip the Internet". IEEE Computer 33(4),12-17 (2000).

[23] Tao Peng, " Defending Against Distributed Denial of Service Attacks", April 2004.

[24] Stefan Axelsson,"Intrusion Detection Systems: A Survey and Taxonomy ",14 March 2000.

[25] stevebauer, davidclark, williamlehr,"understanding broadband speed measurements ", 2008.

[26] j. williampfeiffer," conditions that hinder effective communication ", the pfeiffer library volume 6, 1998.