A HYBRID INTRUSION PREVENTION SYSTEM (HIPS) FOR WEB DATABASE SECURITY

Eslam Mohsin Hassib, IT Engineer, ERG company
Elmahlah Alkobra, Egypt
eslashahassib21@hotmail.com

Aida Osman AbdElgwad
Associate Professor Computer and systems Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt
AOSman@hotmail.com

Ahmed Ibrahim Saleh
Computer and systems Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt
aisaleh@mans.edu.eg

ABSTRACT:

Web database security is a challenging issue that should be taken into consideration when designing and building business based web 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 combination of triple system: (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 Service attacks 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].

It is 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].

Figure 1, demonstrate the general architecture of IDS, which consists of a sensor that monitoring users operations connected to analyzer that analyzing the user behavior and store new detected attacks in IDS database and then send a report to the GUI. The main difference between misuse and anomaly detection is the type of database used. In the misuse detection IDS, the database contains a list of known intrusion techniques or behaviors. On the other hand, in the case of anomaly detection type, the database stores a list of normal user behaviors. In general, misuse detection model cannot detect new, unknown intrusions. Anomaly detection needs to store the records of users' behaviors, which is called “profiles”. The stored profiles are usually large and complex, which needs a large amount of time for detecting an intrusion that takes place a long time ago. Moreover, it is true that neither anomaly detection nor misuse detection can detect Hidden Anomaly.

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 are used, (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.

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 2. 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 2, 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).

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.

![Layered Model](image)

Layer Number | Layers          | Transmitted Data
-------------|-----------------|------------------
7            | Application     | Data             
6            | Presentation    | Data             
5            | Session         | Data             
4            | Transport       | Segments         
3            | Network         | Packets          
2            | Data link       | Frames           
1            | Physical        | Bits             

Figure (2): 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 new namespace 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 domain introduced 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 (3).

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 4; (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].

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. Previous Efforts:

There is relatively little prior work in the field of evaluating intrusion detection systems. The work of Puketza and others at the University of California at Davis is the only reported work that clearly predates the Lincoln effort[22]. These papers describe a methodology and software platform for the purpose of testing intrusion detection systems. The methodology consists of using scripts to generate both background traffic and intrusions with provisions for multiple interleaved streams of activity [23].
These provide a (more or less) repeatable environment in which real-time tests of an intrusion detection system can be performed. Only a single IDS, the network security monitor (NSM), seems to have been tested, and the tests reported could not be seen as any sort of a systematic evaluation. The earlier work, dating from 1993, reports the ability of NSM to detect several simple intrusions, both in isolation and in the presence of stresses[24]. One form of stress is induced by system loading. Load is measured in terms of the number of concurrent jobs running on the host supporting NSM and NSM is reported to drop packets under high load averages (42% byte stream loss at a load average of about 14.5).

Other forms of stress include background noise (non-intrusive network activity), session volume (the number of commands issued during an intrusive session), and intensity (number of concurrent sessions on the link being monitored). No experimental results are given for these forms of stress. In their later paper, the Davis group concentrates on the ability of the test facility to support factoring of sequential attacks into a number of concurrent or overlapping sessions [25].

They report that NSM assigns lower scores to some attacks that have been factored, noting that NSM’s independent evaluation of individual network connections may allow attacks to be hidden in this way. In 1998, while the Lincoln group was developing and carrying out its test methodology, a group at the IBM Research Division in Zurich issued a technical report describing another experimental facility for comparing IDSs [26]. Like the previous work, the Zurich group reports on the design and implementation of a real-time test bed. The Zurich test bed consists of several client machines and several server machines, under the control of a workstation used as the workbench controller. The report discusses a number of issues associated with the generation of suitable background traffic, noting the difficulties associated with alternatives including developing accurate models of user and server behavior, using test suites designed by operating system developers to exercise server behavior, and using recorded “live” data[27].

The authors tend to favor the test suite approach, but recognize that it may bias results with respect to false alarms. Attacks are obtained from an internally maintained vulnerability database that makes hundreds of attack scripts available although only a few are applicable to the initial workbench configuration which only supports FTP services. The article describes several of the attacks on FTP. Considerable attention is given to the controller component of the workbench which allows the systems under evaluation to be configured and administered from a single console. The controller also allows the results from several IDSs to be compared. Unfortunately, the report does not present any results obtained from the workbench.

3. The Proposed Hybrid Intrusion Prevention System (HIPS):

The general structure of the proposed HIPS is illustrated in figure (5). It consists of several modules that will be discussed with the system sequential operations in more details in the following subsections.
3.1. **Host Identity Protocol (HIP):**

As illustrated in Figure (5), the HIP Responder is in the Web server while the clients (host and user) accessing the web database represent the HIP Initiator. 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.

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 that the 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: **DSUC Packet structure:**

<table>
<thead>
<tr>
<th>Next Header</th>
<th>Header Length</th>
<th>0</th>
<th>Packet Type</th>
<th>Version</th>
<th>Res.</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td>controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Sender’s Host Identity Tag (HIT)**

(User’s DSUC)

**receiver’s Host Identity Tag (HIT)**

(Web Server DB Identifier)

**HIP Parameters**

The DSUC packet structure is the same as HIP packet structure as illustrated in figure (6) 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 following three "Res." bits are reserved for future use. The two zero bits in the first line of the header are reserved for potential compatibility. 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 HIP 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):**

It's a server that contain (black list) of banned user identities and MAC addresses, if the user has entered true user ID and password without or with wrong DSUC he will be banned for 24 hours, if the user has entered wrong user ID or password with true DSUC we will give him wrong 5 attempts then he will be banned for 24 hours.

3.3. **Uncertainty degree model (UDM):**

Given a vector of a random variable $X$ and $n$ observations $X_1, \ldots, X_n$, the goal of the statistical sub-model of $X$ is to determine whether a new observation $X_{n+1}$ is abnormal with respect to the previous observations. The mean $\text{avg}$ and the standard deviation $\text{stdev}$ of $X_1, \ldots, X_n$ are defined as shown in Eq. (1):

$$\text{avg} = \frac{X_1 + X_2 + \cdots + X_n}{n}$$

$$\text{stdev} = \sqrt{\frac{\sum_{i=1}^{n} (X_i - \text{avg})^2}{n}}$$  \hspace{1cm} (1)

A new observation $X_{n+1}$ is defined to be abnormal if it falls outside a confidence interval that is standard deviations from the mean, which is denoted by $\text{CI}$ as shown in Eq.(2):

$$\text{CI} = \text{avg} \pm \text{dev} \ \hspace{1cm} (2)$$

Where $\text{dev} = d \times \text{stdev}$ 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 (7) 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. (3):

$$A(t) = \begin{cases} 
1 - (a - t)/\alpha & \text{if } a - \alpha \leq t \leq a \\
1 & \text{if } a \leq t \leq b \\
1 - (t - b)/\beta & \text{if } a \leq t \leq b + \beta \\
0 & \text{otherwise}
\end{cases} \hspace{1cm} (3)$$
Figure (7): Triangular Fuzzy membership function.

Figure (8) 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 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.

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 of databases 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 the rule, the result of the function is calculated as the degree of dubiety.

3.4. System operation:

Figure (9) 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 (9): Flow chart of system operation sequence.
Phase 1: Filtering System check:
- When a new user enters the GUI of the system the system will automatically get its IP address and MAC address from the network hash table and checks them in the blacklist database if its 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 user identity (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 user identity correctly then he will be blocked from the system and his IP and Mac addresses will be added in the blacklist database.
- The blacklist database is cleared every 24 hours.
- If the entered data is correct the user will be allowed to enter the web server database and gets the desired data under certain constrains.
- Now the system will work in two phases in real time, the system administrator will set the monitoring rules of the fuzzy membership function that will be transformed and stored in detection rules base, and the system will monitor the transactions execution and store it in the Analyzer base and monitoring.

Phase 3: Uncertainty Degree Model check:
- The system will uses the fuzzy membership function as shown in Eq. (4) to calculate the degree of uncertainty:

\[
A(t) = \begin{cases} 
1 - \frac{t - \alpha}{\alpha} & \text{if } \alpha - \alpha \leq t \leq \alpha \\
1 - \frac{t - \alpha}{\beta} & \text{if } \alpha \leq t \leq \alpha + \beta \\
0 & \text{otherwise}
\end{cases}
\]  

(4)
- If the Uncertainty degree is high (close to 1) the system will automatically block the user from accessing server database.

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: <AID, UID, 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>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AID</td>
<td>Is the identifier for each Analyzer Record.</td>
</tr>
<tr>
<td>UID</td>
<td>records the user name of the transaction</td>
</tr>
<tr>
<td>SQLTEXT</td>
<td>Records the content of the SQL statement of the transaction.</td>
</tr>
<tr>
<td>Data1</td>
<td>Is the first data field that the transaction relates to, for example; the data value before update.</td>
</tr>
<tr>
<td>Data2</td>
<td>Is the second data field that the transaction relates to, for example; the data value after an update.</td>
</tr>
<tr>
<td>Time</td>
<td>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.</td>
</tr>
</tbody>
</table>

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: <RID, UID, Action, Obj1, Obj2, Condition, Time, Function, Enable>, as illustrated in table (2).
Table (2): Detection Rule structure.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RID</td>
<td>starting with the letter R is the identifier for each detection rule.</td>
</tr>
<tr>
<td>UID</td>
<td>indicates which user the rule is aimed at.</td>
</tr>
<tr>
<td>Action</td>
<td>indicates what type of operations the rule is related to, such as select, update, delete and so on.</td>
</tr>
<tr>
<td>Obj1</td>
<td>is the first object that Action refers to, such as a table, a view or a procedure.</td>
</tr>
<tr>
<td>Obj2</td>
<td>is the second one. If Obj1 is a table or a view, Obj2 will be a field name.</td>
</tr>
<tr>
<td>Time</td>
<td>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.</td>
</tr>
<tr>
<td>Condition</td>
<td>indicates the condition of Action. Usually it is the condition part (where clause) of the SQL statement.</td>
</tr>
<tr>
<td>Function</td>
<td>is sub-tuple recording the information of the membership function used by the rule &lt;α, a, B&gt; Where α, a, and B store the values of α, b, and c respectively (definition of membership function).</td>
</tr>
</tbody>
</table>

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 UID, 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).
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 (10): Eslam Price change chart.

Figure (10) 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 (11): Eslam Uncertainty Degree chart.

The test applied with rules R1, we can see as illustrated in Figure (11) 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.

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

Figure (13): Adel Uncertainty Degree chart.

The test applied with rules R2, we can see as illustrated in Figure (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.
User No.3:

Figure (14): Ahmed Price change chart.

Figure (14) shows us the audit record of operations for a user whose name is Ahmed in 10 days. As we can see as illustrated in Figure (14) that the summation of all changes are \(59-52=7\) > the max no. of changes allowed (5), so he did break the rule, so the user behavior causes anomaly.

Figure (15): Ahmed Uncertainty Degree chart.

The test applied with rules R3. We can see as illustrated in Figure (15) that the user behavior cause anomaly because he did break the rule of 5 euro change, and he made a change of 7 Euro. So, we can notice that the curve has reached the max value (1) which means completely Unacceptable. So, we can see that Ahmed behavior causes anomaly.

4.4.MEASURING SYSTEM DELAY TIME:

In this section, the proposed HIPS is compared with two other systems the first uses a firewall while the other has no security infrastructure. The criteria use for comparison is the delay time versus the number of users. The experiment is established in two different scenarios, the first by measuring the delay time versus the number of normal users 100% (Not Ideal) , while the second measures the system delay time versus the a huge number of hackers and a few normal users.
Figure (16) illustrates the results of the first scenario which measures the system delay time versus the number of normal users. As depicted in such figure, it is shown that the best one is the system with no protection because he hasn't any protection mechanisms, the second one is the firewall system because he has only one security mechanism, finally, and by default our system is the worst one because we use three phases of protection. So, this is a disadvantage of our system.

On the other hand, figure 17 illustrates the results of the second scenario which measures the system delay time versus a huge number of attackers. As depicted in such figure, it is shown that the best one is our system because we use three phases of protection, the second one is the firewall system because he has at least one security mechanism, of course, the worst one will be the system that without protection because he hasn't any protection mechanisms, so the hackers will not have any problem to destroy this system.

5. Conclusion:
We have proposed a new model for web database security using Ultra Hybrid security system based on DSUC and Uncertainty Degree Model. Our tests and experimental results shows that our system is efficient and capable for blocking intruders from hacking into our system and discover suspicious behaviors of internal and authorized system.
users. We can guarantee triple security layers, and test shows that our system can block 93% of attackers on high load.

6. References: