مجلة جامعة النهرين العلوم المجلد ١٥ العدد(٤) كانون الأول، ٢٠١٢ ص 53-58

توفير حماية رصينة لخصوصية وامنية بيانات قواعد المعلومات

عماد عبد الرسول عبد الصاحب
الجامعة التكنولوجية، بغداد، العراق
Imad_sahib@Yahoo.com

الخلاصة

يهدف بحثنا هذا الى توفير حماية رصينة لقواعد البيانات المستخدمة في المؤسسات المختلفة، حيث تعتبر مسألة المحافظة على امنية وخصوصية قواعد البيانات (Database Security And Privacy) من المشاكل المهمة في تطبيقات قواعد البيانات عبر شبكات الاتصالات المختلفة، ومنع نشاطات المتطفلين من غير المخولين (Unauthorized Activity) بالاطلاع على البيانات او التلاعب بها. وتوفير آلية معينة لتسجيل جميع نشاطات المتطفلين، مع الاحتفاظ بتسجيلات كاملة لجميع عمليات تحديث البيانات التي تجري على قواعد البيانات.

كما ويركز البحث على اهمية عملية اختيار كلمات المرور ومفاتيح التشفير، مع امكانية اضافة هياكل بيانات خاصة، واضافة برنامج خاص في بدأ محاولة المستفيد استخدام النظام، لمنع المتطفلين والمتلاعبين بالبيانات منهم، مع منح صلاحيات معينة لكل مستفيد، خلال اوقات محددة خلال يوم العمل والمراقبة المستمرة لاستخدام النظام، والذي يؤدي بدوره في تحسين امنية وخصوصية البيانات.

الكلمات المفتاحية: Database,. LAN Security, Data Encryption, Password, Data Privacy, Data Security.

المقدمة

تعد مسألة المحافظة على امنية وخصوصية قواعد البيانات (*Database Security And Privacy*) من المشاكل المهمة في تطبيقات قواعد البيانات عبر شبكات الاتصالات المختلفة ضد نشاطات المتطفلين من غير المخولين (*Unauthorized Activity*) بالاطلاع على البيانات او التلاعب بها [1] [2]. وتوفير الية معينة لتسجيل جميع نشاطات المتطفلين مع الاحتفاظ بتسجيلات كاملة لجميع عمليات تحديث البيانات التي تجري على قواعد البيانات بعيدا عن ايدي المستفيدين (*Users*) تساعد مدير قواعد البيانات (*Database Administrator*) في تحسين امنيتها وخصوصيتها مستقبلا[3]. وعلية يجب ان تتضمن البرامج المستخدمة في التعامل مع قواعد البيانات التاكيد على امنية وسرية البيانات ومنع الاستخدام الغير صحيح لها بمنح صلاحيات (*Permissions*) معينة وحسب طبيعة ونوعية المستفيد مع المراقبة المستمرة لنشاطات استخدام النظام [4].

توفر معظم تطبيقات قواعد البيانات الحالية (على سبيل المثال *ORACLE*، *SQL Server*) العديد من وسائل الحماية لقواعد البيانات منها (كلمات المرور وتشفير البيانات).

أ-كلمات المرور

جميع تطبيقات قواعد البيانات توفر وسيلة لاضافة كلمات مرور، اضافة الى امكانية المستفيد توفير برامج خاصة به لاستخدام كلمات مرور بعيدا عن كلمات المرور التي توفرها تطبيقات قواعد البيانات [5].

ولاختيار كلمات المرور يجب اتباع الاجراءات التالية :

١. الابتعاد عن الاختيار الاعتيادي لكلمة المرور (مثلا اسم الشخص، تاريخ الميلاد، لقب العائلة، اسم مدير العمل....الخ) حيث يوفر هذا الاسلوب سهولة التخمين.
٢. يتم اختيار كلمات المرور كمزيج من الاحرف والارقام والرموز الخاصة التي توفرها انظمة التشغيل في الحاسبة ويبين المثال التالي عدد الارقام والحروف والرموز الخاصة التي يمكن استخدامها في اختيار كلمات المرور (بالاعتماد على ما توفره اللغة الانكليزية فقط) [6]:

عدد الارقام = ١٠

الاحرف (*Lower/Upper case*) = ٥٢

الرموز الخاصة التي توفرها لوحة المفاتيح = ٣٣

ليصبح المجموع (٩٥) حرف ورقم ورمز خاص يضاف لها جميع الاشكال للحروف التي توفرها اية لغة ما عدا الانكليزية ليصبح مجال الاختيار واسعا جدا.

٣. يفضل ان يكون طول كلمة المرور لا يقل عن ١٠ (حرف او رقم او رمز خاص) والجدول التالي يبين الفترة اللازمة لتخمين كلمة المرور [6] :

عدد الاحرف المستخدمة	عدد المحاولات	الوقت اللازم
٤	١٠ مليون	١.٦ ثانية
٦	١٠ مليون	1.9 ساعة
٨	١٠ مليون	٣٢٦ يوما
١٠	١٠ مليون	٣٦٠٠ سنة

٤. امكانية اختيار اكثر من كلمة مرور للمستفيدين المهمين (مثلا مدير قاعدة البيانات) [7].

٥. اهمية اختيار كلمات مرور صلاحيتها مرتبطة بالتوقيت خلال اليوم.

ب –تشفير البيانات (*Data Encryption*)

اجراءات تشفير البيانات[8][9] (*Data Encription*) تتضمن تشفير كلي للبيانات او تشفير جزئي (*Partial Encryption*) حيث يتم تشفير جزء من البيانات بحيث لا تتيح للمتطفلين عبر شبكات الحاسبات المختلفة [9] امكانية معرفة طبيعة البيانات من خلال حجب هذه البيانات وهياكل البيانات المستخدمة عنهم، ومثال على ذلك تشفير جميع المفاتيح الرئيسية والثانوية في جداول هياكل البيانات المستخدمة. وتتم عملية التشفير باستخدام مفتاح تشفير (*Encryption key*) ومن الممكن استخدام اكثر من مفتاح لتشفير البيانات وحسب اهميتها. وتخضع ضوابط اختيار المفتاح الى نفس الضوابط الخاصة باختيار كلمة المرور.

من خلال متابعة الانظمة المنفذة في اية مؤسسة بعد التحول من انظمة منفذة على حاسبة واحدة (مستفيد واحد فقط) الى انظمة اعتمدت مبدأ (الخادم والمستفيد) مع الاحتفاظ بهياكل البيانات والبرامج (السابقة بدون تغيير)، برزت المشاكل الامنية التالية [10] [11]:

١. باستطاعة كل مستفيد ضمن الشبكة استعراض وتحديث جميع جداول النظام بدون تدوين ما قام به المستفيد وما هي طبيعة المعلومات التي تم تغييرها (اي وجود فرصة للتلاعب بالبيانات دون ترك اثر لذلك).

٢. يمكن استخدام احدى الحاسبات المرتبطة بالشبكة لتغيير جميع هذه البيانات وفي اي وقت يكون فيه الخادم في حالة اشتغال.

ويهدف البحث الى دراسة هذه المشاكل الامنية اعلاه من خلال نظام الرواتب المطبق في مؤسسات الدولة المختلفة وايجاد الحل المناسب لها.

الطرق العملية

أ – نظام رواتب منتسبي الدولة

يعد نظام الرواتب احد الانظمة الادارية المتوفرة في كل مؤسسات الدولة والشركات ومنذ البدأ بالاستعانة بالحاسبة في مكننة الاعمال الادارية و يختص بالمعلومات الحسابية الخاصة بالمنتسب.

أ–١: نبذه تاريخية

بصورة مبسطة يتكون النظام من تصميم الشاشات وكتابة البرامج اللازمة للتنفيذ من شاشات الادخال، شاشات التحديث وادامة المعلومات الى استخراج التقارير المطلوبة، اضافة الى الجداول (هياكل البيانات) التالية:

- جدول المعلومات الاساسية (اسم المنتسب، رقم المنتسب، الشهادة، نوع المنتسب، الراتب الشهري...لخ).
- جدول المخصصات (رقم المنتسب، نوع المخصصات، مقدار المخصصات..... الخ).
- جدول الاستقطاعات (رقم المنتسب، مقدار الاستقطاعات، رقم القسط..... الخ).
- جدول الفروقات الشهرية (رقم المنتسب، مقدار الفروقات، نوع الفروقات..... الخ).

والجداول اعلاه هي جداول كلاسيكية مستخدمة تقريبا مع جميع انظمة الرواتب المعتمدة في مؤسسات الدولة المختلفة.

بصورة عامة تتكون فئات منتسبي مؤسسات الدولة والتي يتعامل معها نظام الرواتب مما يلي:

- الحرفيين.
- الاداريين.
- الفنيين.
- المهندسين.
- التدريسيين.

ومن اجل التغلب على المشاكل الامنية التي تم ذكرها في المقدمة تم استخدام عدد من هياكل البيانات (جداول).

ب – هياكل البيانات المستخدمة :

ب – ١ : هيكل البيانات المستخدم لخزن معلومات المستفيد وصلاحياته.

يتكون هيكل البيانات الخاص بصلاحية المستفيدين من الحقول التالية :

جدول رقم (١)

صلاحية المستفيد.

ت	اسم الحقل
١	*IP Address*
٢	اسم المستفيد (*User Name*)
٣	كلمة المرور الاولى (*Password١*)
٤	كلمة المرور الثانية (*Password2*)
٥	الصلاحية
٦	وقت بدأ الصلاحية
٧	وقت انتهاء الصلاحية

مع ملاحظة انه تم اختيار مبدأ (الـ*IP address*) بدلا من *MAC address* لتسهيل استبدال الحاسبة في حالة عطلها. وهنا استخدم مبدأ كلمة المرور المرتبطة بالوقت (تستخدم ساعة الخادم لتحديد الوقت) لمنع استخدام النظام من قبل المتطفلين خلال ايام العطل او بعد الدوام الرسمي، كما تم مراعاة اختيار كلمات المرور لتكون من الصعوبة استنتاجها (كما جرت العادة اسماء اشخاص او مسؤولي الدائرة او تاريخ اعياد الميلاد.....الخ) ولا تكون قصيرة (اختيرت كلمة المرور لتضم ١٢- ١٤من الاحرف والارقام والرموز الخاصة) اما مدير القاعدة (*Database Administrator*) فيمتلك جميع الصلاحيات وفي جميع الاوقات مع استخدام كلمتين (٢) مرور عند استخدامه النظام اما بقية المستفيدين فكلمة مرور واحدة فقط والثانية فارغة.

ب-٢ : هيكل البيانات الخاص بمتابعة تغيير المعلومات(تحديث، حذف، اضافة) :

يتكون من الحقول التالية:

جدول رقم (٢)

متابعة التغييرات التي تطرأ على المنتسب.

ت	اسم الحقل
١	رقم الحاسبة
٢	رقم المنتسب
٣	نوع التحديث
٤	تاريخ التغيير
٥	وقت التغيير
٦	اسم الحقل المعدل
٧	القيمة السابقة للحقل
٨	القيمة الجديدة للحقل

ب-٣ – جدول البيانات الخاص بمتابعة المتطفلين ويتكون من الحقول التالية:

جدول رقم (٣)

متابعة المتطفلين على النظام.

ت	اسم الحقل
١	رقم الحاسبة
٢	اسم المستفيد
٣	تاريخ محاولة الدخول
٤	وقت محاولة الدخول

مع التاكيد على الابتعاد عن الارتباط بشبكة الانترنت (طبيعة العمل لا تتطلب ارتباط الحاسبات بشبكة انترنت).

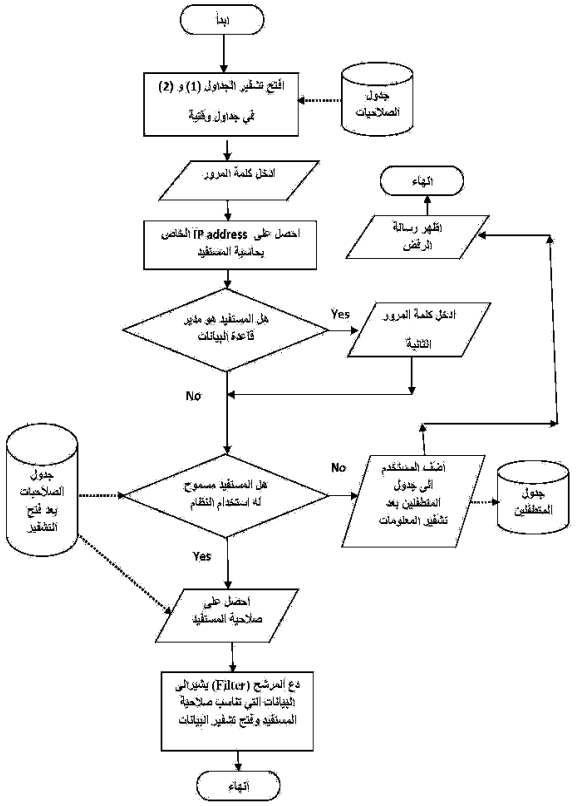
ومن خلال الجداول اعلاه تكون واجهة البدء باستخدام النظام كما هي موضحة في الشكل (١).

ومن خلال الجدول (٢) اعلاه نلاحظ امكانية استعراض جميع التغييرات التي حدثت لمنتسب معين خلال جميع الفترات السابقة وتكون مرتبه (*sorted*) حسب التاريخ والوقت تنازليا (من الاحدث الى الاقدم). والجدول (٣) اعلاه يوفر امكانية معرفة المتطفلين على النظام ومعلومات عن الحاسبة ووقت وتاريخ التطفل.

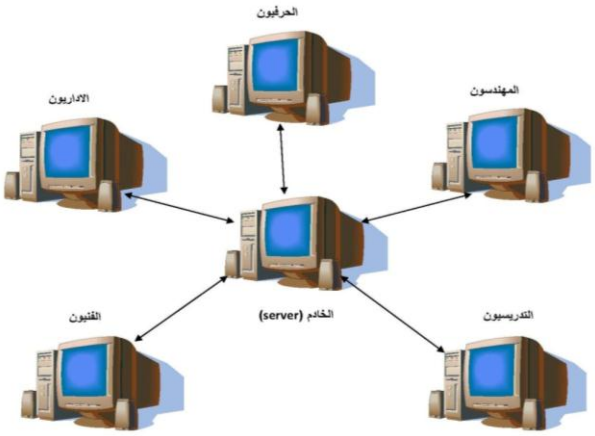
علما ان الجداول(١، ٢ و ٣) اعلاه غير متاحة للمستخدم نهائيا لانها توضع في مجلدات خاصة في الخادم وبعيدا عن متناول المستفيد والمتطفلين ولا يمكن الاطلاع عليها او تحديثها الا من قبل مدير قاعدة البيانات مع انها بالاساس مشفرة (*encrypted*).

ج – تاسيس الشبكة المحلية (*LAN*)

من خلال تخصيص العمل لكل حاسبة بفئة معينة من المنتسبين(اي ان هناك حاسبة معينة خاصة بالحرفيين.... الخ). كما في الشكل (٢) ومن خلال ما ذكر اعلاه تم التغلب على مشكلة المتطفلين على النظام والمتلاعبين بالمعلومات (امنية وخصوصية البيانات *Security and Privacy*). ومن خلال مراقبة تطبيق اسلوب هذا البحث وهياكل البيانات المقترحة على نظام الرواتب في الجامعة التكنولوجيةخلال فترة عام ٢٠١٠ و الربع الاول من عام ٢٠١١، تم رصد بعض محاولات الاختراق الفاشلة في استخدام النظام كما تم تحديد المسؤولين عن تغيير بيانات المنتسبين في حالة الحاجة الى ذلك. والجداول (٤، ٥) يوضح بعض النماذج التطبيقية تم استنباطها من هيكل البيانات الخاص بمتابعة تغيير المعلومات الخاصة بنظام الرواتب وهيكل بيانات المتطفلين وقد تم استخدام اسماء مستفيدين وارقام حاسبات وهمية للمحافظة على امنية المعلومات الحقيقية.



شكل (١) مخطط السيطرة على صلاحية المستفيد واستخدام النظام.



شكل (٢) مخطط شبكة نظام الرواتب.

جدول رقم (٤)

تحديد المتطفلين.

اسم المستفيد	*IP ADDRESS*	تاريخ محاولة الدخول	وقت محاولة الدخول	الملاحظـات
مستفيد ٣	192.168.0.7	٢٠١١/٣/١٥	١٢:١٠:٠٣ ص	كلمة المرور خطأ
مستفيد ٢	192.168.0.5	٢٠١١/٣/١٥	٠٩:١٠:٠٣ ص	غير مخول بالاطلاع على بيانات التدريسيين
مستفيد ١	192.162. 0.20	٢٠١٠/٢/١٧	٩:١٠:١٤ ص	عدم وجود لاسم المستفيد في الجدول (١)

جدول رقم (٥)

تحديد المسؤولين عن تغيير بيانات المنتسبين.

رمز الحاسبة	نوع التحديث	وقت التحديث	تاريخ التحديث	رقم المنتسب	اسم الحقل	القيمة القديمة	القيمة الجديدة
192.168.0.7	اضافة قيد المخصصات	١٣:١٠:٠٤ ص	3/3/2011	131415	رمز المخصصات مبلغ المخصصات تاريخ الاستحقاق		9 20000 02/01/201
192.168.0.1	اضافة قيد استقطاعات	١٣:١٠:٠٤ ص	2/27/2011	130994	رمز الجهة الدائنة مبلغ السلفة مبلغ القسط رقم القسط الرصيد المتبقي		8 25000000 57900 3 24826300
192.168.0.1	تعديل قيد المخصصات	١٠:٣٠:٠٤ ص	2/24/2011	126889	رمز المخصصات مبلغ المخصصات تاريخ الاستحقاق	11 119685 24/10/2010	11 91245 24/10/2010
192.168.0.47	تعديل قيد معلومات عامة	٠٩:٠٤:١٥ ص	2/22/2011	126877	تاريخ الترفيع الدرجة الفئة الراتب الشهري	01/01/2010 3 7 693000	2010/11/09 2 1 758000
192.168.0.47	اضافة قيد فروقات	٠٩:٠٣:٣٧ ص	2/22/2011	126877	نوع الفروقات مبلغ الفروقات تاريخها		1 119466 ٢/١٠/٢٠١١

المناقشة

من خلال بحثنا هذا اوضحنا اهمية المحافظة على امنية وخصوصية بيانات قواعد المعلومات عبر شبكة من خلال توضيح اهمية الية اختيار كلمات مرور (صلاحيتها مرتبطة بالتوقيت خلال اليوم) ومفاتيح التشفير، وما لها من دور بابعاد المتطفلين على المعلومات، ومراقبة المتلاعبين بالمعلومات من خلال عدد من هياكل البيانات تم اضافتها لما هو موجود اصلا، اضافة الى مخطط انسيابي لبرنامج يضاف الى واجهة بدء المستفيد باستخدام النظام، والتي من خلالها تم منع ورصد ومتابعة العديد من المخالفات من قبل المتطفلين والمستفيدين واتخاذ الاجراءات المناسبة حيال ذلك.

مع التاكيد على اهمية ان تكون هياكل البيانات في الجداول المشار اليها في البحث غير متاحة للمستخدم نهائيا لانها وضعت في مجلدات خاصة في الخادم وبعيدا عن متناول المستفيد والمتطفلين، ولا يمكن الاطلاع عليها او تحديثها الا من قبل مدير قاعدة البيانات، والتاكيد على تشفيرها.

وقد تم تطبيق النماذج المقدمة في بحثنا هذا واستخدامها في نظام الرواتب في الجامعة التكنولوجية، مع التاكيد على عدم الحاجة عند تطبيق هذا النموذج الى اعادة توصيف هياكل البيانات المستخدمة او اعادة كتابة برامج النظام فيما عدا اضافة الاسلوب المستخدم في بحثنا هذا في واجهة دخول المستفيد الى النظام.

الاستنتاجات

اثبت بحثنا هذا فعالية كبيرة من خلال تجربة تطبيقه على نظام رواتب منتسبي الجامعة التكنولوجية، من خلال:

- المراقبة المستمرة للاستخدام لفترة امتدت لـ ١٥ شهرا.
- اجراء محاولات تجريبية من قبلنا للاختراق حيث تم رصدها عند التغييير على البيانات، ومنعها في حالة عدم وجود صلاحية (استخدامه كجدار ناري *Fire Wall*).
- منع محاولات استخدام نظام الرواتب من قبل المتطفلين، ومتابعة مستمرة عند تغيير المعلومات من قبل المخولين، والرجوع اليها عند الحاجة.
- امكانية اضافة اسلوب البحث هذا الى اي نظام منفذ حاليا بسهولة، للسيطرة على المتطفلين والمتلاعبين بالبيانات، وبدون احداث اي تغيير يذكر على برامج النظام او هياكل بياناته.

المصادر

[1]Samba Sesay, Zongkai Yang, Jingwen Chen and Du Xu, "A Secure Database Encryption Scheme", Consumer Communication and Networking Conference, IEEE, Volume 2, pp49-53, 2005.

[2] Ahmed M.A. Al thneibat1, Bahaa Eldin M. Hasan2, Abd El Fatah. A. Hegazy3, Nermine Hamza4, "Secure Outsourced Database Architecture", IJCSNS International Journal of Computer Science and Network Security, VOL.10, pp246-253, 2010.

[3] Liu, S. , Kuhn, R., "Data Loss Prevention", IT Professional, Volume 11, pp10-13, 2010.

[4] Lv Guangjuan , Xu Ruzhi , Zu Xiangrong , "Information Security Monitoring System Based on Data Mining International", 2009 Fifth International Conference on Information Assurance and Security, IEEE, Volume 1, pp472-475, 2009.

[5] Sharma, A. , Ojha, V. , Belwal, R.C. , Agarwal, G., "Password based authentication: Philosophical survey",: 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems ,IEEE,Volume 3 ,pp619-622 , 2010.

[6] Bernie Thomas, "Simple Formula for Strong Passwords (SFSP)", http: //www.sans.org/reading_room/whitepapers/authentication/simple-formula-strong-passwords-sfsp-tutorial_1636 , 2005.

[7] Yang Jian, "An Improved Scheme of Single Sign-On Protocol Based on Dynamic Double Password", 2009 International Conference on Environmental Science and Information Application Technology , IEEE , Volume 3 ,pp572-574, 2009.

[8] Zhao Yong-Xia, "The Technology of Database Encryption ", Second International Conference on Multimedia and Information Technology, IEEE, Volume 2, pp268-270, 2010.

[9] F. Vancea,C. Vancea, "Protecting data integrity with chained rows and public key cryptography", Journal of Computer Science and Control Systems , Volume 1, pp114-117, 2008.

[10] Navleen Kaur, Dr. Amardeep Singh, Sarabpreet Singh;"Enhancement of Network Security Techniques using Quantum Cryptography";: International Journal on Computer Science and Engineering, Volume 3 , pp1960-1964 , 2011.

[11] Marin, G.A., Network Security Basics", IEEE security & privacy, Volume 3, P68-72, 2005.

Abstract

This research designed to provide many solid rules to protect the database used in different database applications, where is the question of maintaining the databases security and privacy which is an important problems in database applications across networks of various communication and prevent the activities of hackers from unauthorized access to data or manipulate it. Also to provide a specific mechanism to record all activities is being maintained with complete recordings for the data operations that take place on the databases.

It also focuses on the importance of the process of selecting passwords and encryption keys with the possibility of adding specific data structures with the addition of a special program in the start try the beneficiary to use the system to prevent hackers and manipulators of data, including giving certain permissions to each beneficiary during specific times during the working day and ongoing monitoring of the use of the system, which lead role in improving the security and privacy of data.