Securing Electronic Medical Record and Electronic Health Record Systems through an Improved Access Control

Pasupathy Vimalachandran, Hua Wang, and Yanchun Zhang
Centre for Applied Informatics
College of Engineering and Science
Victoria University, Melbourne Australia

Pasupathy.Vimalachandran@live.vu.edu.au
{hua.wang,yanchun.zhang}@vu.edu.au

Abstract

During the last two decades, modern technology is increasingly being used in the healthcare sector in order to enhance the quality and the cost efficiency of the healthcare services. In this process, Electronic Medical Record (EMR) has been introduced to collect, store and communicate patient's medical information. The EMR systems enable efficient collection of meaningful, accurate and complete data to assist improved clinical administration through the development, implementation and optimisation of clinical pathways. While its cost and time savings are encouraging for transition, it does not come without inherent challenges. Inadequate policy development in the areas of data security and privacy of health information appear to be the major weakness. In this paper, we present a secure access control model for the EMR and Electronic Health Record (EHR) to provide acceptable protection for health sensitive data retained at healthcare organisations. We systematically analyse four existing access control mechanisms that have been proposed in the past, and present a combined more secure model for the EMR and EHR for healthcare provider organisations in Australia.

Categories and Subject Descriptions
Security and protection – access control

General Terms
Security, Access Control, EMR, EHR, PCEHR

1. Introduction

25 years ago, patient records were on 8 x 5 inch cards, receipts were done using the Kalamazoo system, suture material was okay to reuse if soaked in antiseptic solution, and the only transfer of information was by telephone or mail [1]. Times have now changed. 98% of general practitioners now have a computer on their desk and 70% to 94% use computers to the level of regularly documenting progress notes/clinical records [2]. In most parts of the developed world, healthcare has evolved to a point where patients have more than one healthcare provider. This may include general practitioners, specialists, allied health services and hospitals to service their diverse medical needs. As a result, medical records have been found scattered throughout the entire healthcare sector, from primary care - general practices and clinical laboratories, to pharmacies and specialist practices. This has resulted in the growing need to create an integrated infrastructure for the collection of diverse medical data for healthcare professionals, where the adoption of standardised Electronic Health Record (EHR) has become imminent.

The distinction between EMR and EHR can be quite confusing. The EMR consists of electronic information about a patient recorded in an individual clinic, and performs a similar function to that previously performed by the paper record. The EHR, on the other hand, is a summary of health events (usually drawn from several EMRs) and may consist of the elements that are eventually shared in a national EHR [1]. An online EHR enables patients to manage and contribute to their own medical notes in

a centralised way which greatly facilitates the storage, access and sharing of personal health data. It is clear that storing medical records digitally on the cloud offers great promise for increasing the efficiency of the healthcare system. As a result, a national EHR was introduced to Australia in 2012 and the Government has invested $467 million to build key components of the Personally Controlled Electronic Health Record (PCEHR) to improve health outcomes and reduce costs in the country [3].

The setting up of the PCEHR system faces many challenges which ultimately impede its wider adoption. Privacy and confidentiality of patients' health information is crucial. Once patients' personal health data are stored in the cloud or local server with EMR or EHR, it is not quite clear who else can access it other than the patient's usual doctor. For example, with the current system, in a healthcare provider organisation, all other healthcare providers working for the organisation can access patient clinical information. There are also instances where administration staff may access patients' clinical information for improving the business (e.g. targeting chronic disease high risk or pap smear patients who are due for a reminder).

Healthcare organisations are inherently complex and dynamic environments [4], [5] which makes it difficult for administrators to define access control policies [6]. EMR and EHR user privileges are therefore often defined at a coarse level to minimise workflow inefficiencies and maximise flexibility in the management of a patient. The consequence of such practice is that EMR systems are left vulnerable to potential abuse from insiders who are authenticated within the organisation, which ultimately can compromise patient confidentiality. Furthermore, Information Technology (IT) technical staff or the system operators who maintain the IT systems and the databases also may access patients' clinical information. This leads to risk of intentional or unintentional leakage, despite privacy and confidentiality agreements. However, these agreements do not eliminate leaks occurring, they mitigate the risk, based on the person's professional integrity. This demonstrates that information stored in EMR and EHR databases or cloud servers face significant risk of exposure. This potential for internal abuse must be addressed. It is also important to acknowledge and investigate these challenges and shortcomings associated with the current electronic health information system and determine possible solutions to ensure its wide adoption and success of the PCEHR system in Australia.

In this paper, we discuss four different existing access control strategies and eight different spectrums of attack or misuse that have been identified in the past and we present a combined and improved access control mechanism with a security model to the health industry.

2. Related work

There are different access control strategies for EHR and EMR that have been developed in the past [4].

According to one Forrester study, 80% of data security and privacy breaches involve insiders, employees or those with internal access to an organisation, putting information at risk [5]. With health sensitive data, this risk becomes more prominent. Many researchers have proposed various resolutions to solve the security and privacy problems associated with the EMRs and EHRs. These problems mainly refer to access control. The term "access control" is simply defined as "the ability to permit or deny the use of something by someone" [5]. The key objective of access control mechanisms is to permit authorised users to manipulate data and thus maintain the privacy of data [6]. There are different access control mechanisms that have been identified in the literature review. The basic models of the access control principles are i) Discretionary Access Control (DAC), ii) Mandatory Access Control (MAC), iii) Role Based Access Control (RBAC) and iv) Purpose Based Access Control (PBAC). However, the development is not satisfactory enough to fulfil the privacy requirements of EMRs and EHRs [7].

DAC uses access restriction set by the owner and restricts access to the objects. However a user who is allowed to access an object by the owner of the object has the capability to pass on the access right to other users without the involvement of the owner of the object [8]. Because of this granting, read access transitive, the policies are open for Trojan Horse Attack [9].

MAC is a set of security and privacy policies constrained according to system classification, configuration and authentication. The policies made

by a central authority [10]. Compared to DAC, MAC policy can prevent a Trojan Horse Attack and the integrity of the data objects can be protected by using the "Read Up" and "Write Down" Rules. In MAC, the individual owner of an object has no right to control the access. Therefore, MAC policy fails to preserve the privacy requirement for EHRs of the patients [11]

In RBAC [9], each user's access right is determined based on user roles and the role-specific privileges associated with them. RBAC policy uses the need-to-know principle to assign permissions to roles and to fulfil the least privileged condition by the system administrator. However, RBAC does not integrate other access parameters or related data that are significant in allowing access to the user [12]. PBAC is based on the notion of relating data objects with purposes [13]. Many researchers have identified that greater privacy preservation is possible by assigning objects with purposes [14]. However, Al-Fedaghi describes [15] that PBAC leads to a great deal of complexity at the access control level.

In addition to access control mechanisms, it is also important to identify the spectrum of attacks or misuse that could be performed by attackers. A wide range of attacks have been documented in the literature. It is essential to know the different possible attacks for health based databases, in order to design a suitable health data security system. To achieve this goal the literature review has been performed to discuss different main attacks that health based databases currently face.

In the British Computer Society website at http://www.bcs.org/server.php?show=ConWebDoc.8852, Amichai Schulman and Imperva say "enterprise database infrastructures, which often contain the crown jewels of an organisation, are subject to a wide range of attacks" [16].

A review of previous attacks has revealed the following main methods utilised to obtain sensitive health information.

1. Excessive privilege granted to staff
2. Privilege abuse
3. Unauthorised privilege elevation
4. Platform vulnerabilities
5. SQL injection
6. Weak audit
7. Weak authentication
8. Exposure of back-up data

With excessive privilege, healthcare organisation application users are granted privileges that may exceed the requirements of their role. As an example, a reception/ administrative staff member whose job requires name, contact details and time of the appointments of a patient, may be able to view clinical notes of patients.

Healthcare application users may abuse legitimate data access privileges for unauthorised purposes. This is known as 'privilege abuse'.

Unauthorised privilege elevation means that the attackers may take advantage of vulnerabilities in health based cloud software systems to convert low-level access privileges to high-level access privileges. For instance, an attacker may take advantage of cloud based system buffer overflow vulnerability to grant administrative privileges.

Platform vulnerability is taking advantage of the vulnerabilities in underlying operating systems, which may lead to unauthorised data access or corruption. The blaster worm took advantage of a Windows 2000 vulnerability to take down target servers [17].

Users may take advantage of vulnerabilities in front-end web applications and stored procedures to send unauthorised database queries. This is known as "SQL injection".

Weak audit policy and technology represents risks in terms of compliance, deterrence, detection, forensics and recovery. In other words, the cloud based health system software provides weak audit solutions itself. These products very rarely log the detail about what application was used; the source IP address and what queries failed.

Weak authentication allows attackers to assume the identity of legitimate database users. Most of the time, the users use their name, personal identification, meaningful words or plain text as a password.

In most situations, people protect the main cloud based health database, not actual back-ups. With exposure of back-up data, attacks have involved theft of database backup tapes and hard disks.

3. Secure EMR and EHR through an improved access control mechanism

The system operator of the PCEHR who manages the system or practice staff in a healthcare provider organisation, may intentionally leak patients' clinical information. The access control currently in use does not prevent this kind of breach.

In a healthcare provider organisation or an organisation that manages an EHR system, it is not clear who accesses what information in that organisation. In a general practice (medium or large) environment in Australia, organisations normally use two types of software systems to deal with patients. One is the Patient Management System (PMS) that assists with appointment and billing related tasks. This is also known as the 'billing system'. The other is for managing clinical tasks and information and is called the 'clinical system'. Most general practice software systems are integrated with both tasks. In some cases, the same product has two software systems which are compatible and work together. If an organisation uses different software systems for billing and clinical, then assigning access control is easier. For instance, reception staff have access to the billing system and not the clinical system. On the other hand clinicians including doctors and nurses access both clinical and PMS but not billing. However if an organisation uses an integrated one system for both billing and clinical, then the issues associated with access control becomes complicated. However there are situations, where healthcare organisations manage this issue by giving permission levels based on the roles and purposes. These permission controls are managed by the software itself.

In healthcare organisations, there are non-clinical staff, such as administration staff who may need to access clinical related information to target patients to increase the organisation's business. For example; the practice follows up with health checks due and reminds mainstream patients or identified chronic disease high risk patients of the need for consultations. In these circumstances, administration staff may access clinical information. This access may lead to internal abuse. Therefore, administration staff accessing clinical information is a risk. However, considering the financial benefit to the organisation, it cannot just be ignored. Hence the access must carefully be monitored and controlled to maintain the privacy and confidentiality of patients to mitigate this risk.

The healthcare organisation's software systems use DAC and MAC access control principles. RBAC is also used in those systems however PBAC is not in use in many healthcare systems because of the complexity at the access level. Furthermore, considering the current privacy and security issues associated with health records, a single access control principle is inadequate to protect the highly sensitive information. Thus, it is crucial to use a combination of more than one access control principles in this environment. When administration staff access clinical information from the system where RBAC is switched on, the purpose of the access is not mentioned. To solve this issue, an authorisation from an authority must be given to access the information. Then a combination of RBAC and PBAC must be applied for a secure access. This means, if an administration staff wants to access the clinical information, a high level management staff must give permission every time. High level management staff might be a doctor or a nurse or practice manager who has high level privilege to access all parts of the health record. This will require both access control principles RBAC and PBAC for access.

In computer security, access control covers authentication, authorization and audit. Access control systems provide the important services of identification, authentication, authorization and accountability to enter into an application or system. Identification and authentication determine who can log into a system (the system may be an application or even an operating system). Authorization provides different privileges for a system (usually categorized high-level, medium-level and low-level) in accordance with employee's role in a healthcare organisation. Finally the accountability identifies the subject a user worked on during his or her log-in.

The Security Engineering Guide (SEG) explains the term as "Access control is the traditional centre of gravity of computer security. It is where security engineering meets computer science" [18].

The security engineering guide also discusses how the access control works at a number of levels and describes the following different levels in Figure 1.

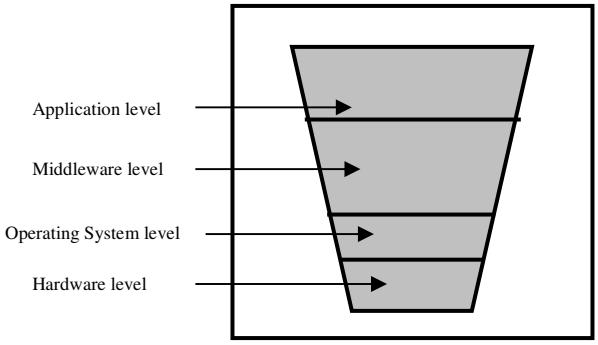


Figure 1: *Access controls at different levels in a system* [18]

Authentication, authorization and audit ability and their levels of permission vary on different levels of access control for a system.

4. Proposed model ("HighSec system")

After considering several aspects of access control mechanisms through literature research, it was realized that there is a real need to put more control on this level of security. This led to developing a mechanism called "log-in pair" which will be an ideal answer to minimise the potential for misuse or abuse of health data within a healthcare organisation. If this concept can be followed with well-planned pair design within a healthcare organisation, it will be one of the better options for maintaining high security.

In many instances, health sensitive and confidential data (e.g.; clinical notes / medical conditions) are stored in databases of clinical software systems. These data are susceptible to internal abuse as they can be viewed by anyone in the internal setting. Hence this sensitive data needs to be protected from internal abuse. The "log–in pair" is a technique which may achieve this objective.

Log-in pair: To access data through this system, an employee who has top level privilege (super user) has to give authorisation to a user to access health sensitive data. Hence, the super user keeps track of what the user does with the sensitive data. Every user is made aware that once they log in, the super user follows them, and keeps track of what is being accessed. It is like a counter check. The responsibility and the accountability are shared. This concept will ensure high security.

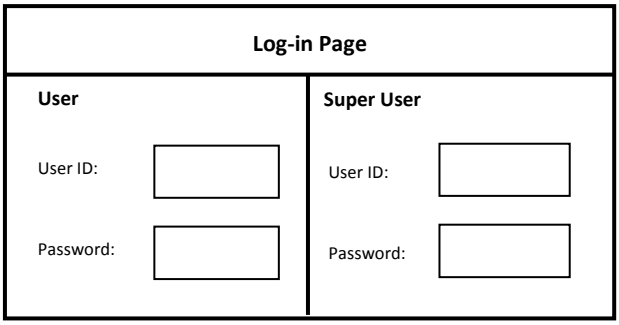


Figure 2: *Sample log-in page*

When the pairs are set-up, the following main factors need to be considered; the physical location of the users and super users (e.g.; sharing the same office), job discipline of users (employees who are working in a similar discipline are paired) and the frequency and time an employee enters and uses the system (e.g.; an employee who needs to use the system for the whole day, all seven days a week should be paired with another employee who also uses the system for the whole day, all seven days a week rather than with an employee who only needs to access the system for a few hours in a week).

As Figure 2 illustrates, every user has his or her own individual user id and password to enter into the system. In this pair log-in concept, see table 1 below, for user A to enter into the system the super user D should enter his or her user id and password as well. Consider a healthcare organisation with three users (A, B and C) and three super users (D, E and F).

Table 1: *Basic pair design*

Pair	**Users & Super Users**
1	A & D or E or F
2	B & D or E or F
3	C & D or E or F

The log-in page must be designed to accept inputs for two users with separate user identification and password.

The security assurance in this system is that one person cannot function on his or her own. If one user

wants to enter into the system, he or she must be given super user permission. Hence, it mitigates users abusing the system.

This system has its own problems:

1) If all super users are absent (from above example, if D, E and F are on leave) a user cannot enter into the system or perform routine jobs.
2) The system cannot prevent both user and super user as a pair deciding to abuse the data.
3) Having someone else to log in the same time as another user creates potential sources of bottleneck and make user frustrated with the system.
4) If doctors and nurses are potential "gatekeepers" (the authoring login), these professions are already extremely busy, and likely to create users circumventing the system.
5) If authorising persons consistently logon and give the login credentials to users, then this defeats the aim of the system.

To overcome the first problem, a super user may be able to give permission through the internet or networking as a future development. Alternatively doctors will also be considered as super user who can give permission for users to work on sensitive data.

However, it is very difficult to overcome the second problem. A system monitoring facility may be developed as a part of this system to monitor the users and super users. A system audit and/or quality improvement process may mitigate this risk.

The system itself must be notified and does not give access to other users to avoid bottlenecks and unnecessary delays in logging on the system over the network at that point in time.

In practice, doctors and nurses are extremely busy and difficult to contact to gain their login in order to access the system. However, they are the people who have got authorisation to access clinical information in healthcare organisation environment. To resolve this issue in creating users circumventing the system, alternative non-clinical top level staff can be appointed (i.e.; practice manager, assistant practice manager).

Super user authorisation is a crucial part of this method. Therefore login credentials of super users must be strong and changed periodically. Considering super users availability, the system can be configured to send an auto creating password to the super user through email or as a text message to mobile phone weekly. One option may be that the super user can login to the system using their member password (which is different to authorisation password) and view the weekly authorisation password.

5. Construction of the proposed model

When designing the pairs, the healthcare organisation internal workflow, organisation chart and the management inputs can also be considered. The log-in page must be designed to accept inputs for two users with separate user identification and password.

This can be accomplished using the same computer or different computers which are networked. The users should log-in one after another within 90 seconds. If the second user fails to login within 90 seconds of the first user logging-in, the permission to enter into the system will be refused.

The following specification and Figure 3 explain the construction of the proposed model.

Specification:

1. *Item – text box. Input into user_pw.u_id.*
2. *Item – text box. Input into user_pw.u_pw*
3. *Item - check box. Value (Y/N). If Value = 'Y' open Block 2 and enable. If value ='N' hide Block 2.*
4. *Item - push button. On press open the main form.*
5. *Item – push button. On press exit from the application*
6. *Item – text box. Input into Block2.new_password.*
7. *Item – text box. Input into Block2.confirm_password.*
8. *Item - push button.*
   On press check that, if (New password = confirm password)
   alter table user_pw
   setu_pw = new_password;
   commit change.
9. *Item - push button. On press clear item new_password, confirm_password.*
   Hide block 2.

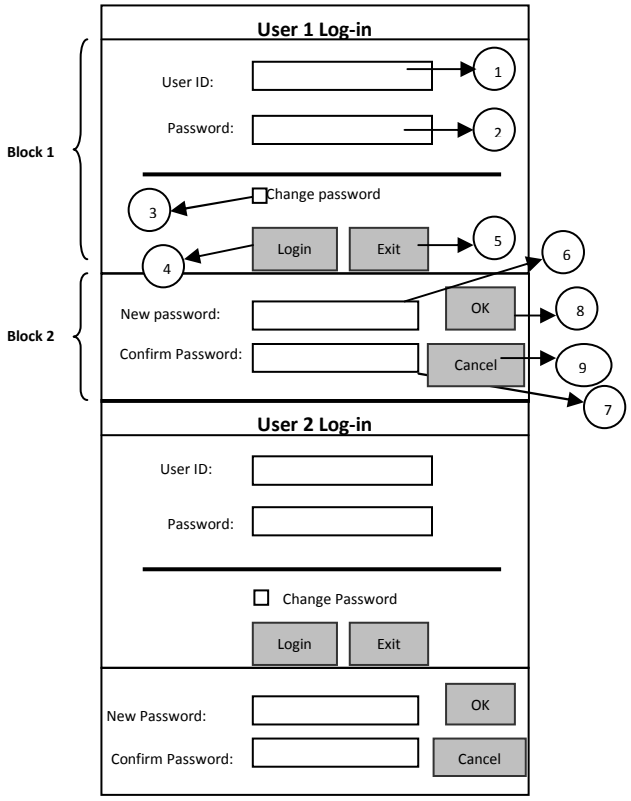


Figure 3: *Designing log-in pair interface*

6. Conclusion and future suggestions

In this paper, we have introduced a new concept called 'log-in-pair' in access control. Even though access control is the first and basic security level for any computer system, it is important to make sure that the level of protection is high. This may be an ideal answer to minimise misuse or abuse within healthcare organisations. Though the proposed method seems easy to implement, in practice, there will be more concerns when this concept is in progress.

However, we are sure, if this concept could be followed with well-planned pair designing through education, policies and procedures within an organisation, it would be one of the better solutions in maintaining and practicing a high security system in a healthcare environment.

Log-in pair, the concept sounds good, but needs additional consideration in making pair users. There are number of factors/criteria that should be developed to satisfy this level of security. The physical location of the user of the pair user, discipline of the user, work load and purpose are some of them. A System Monitoring Facility (SMF), with log-in pair, which will observe the user activities with the EMR and EHR systems, and log audits after a user has entered into the system. This kind of SMF would definitely be beneficial in increasing the level of security for access control. Hence, an appropriate policy and procedure documentation in creating user pair and a SMF in monitoring users' could be considered for future development. Multiple login and logout over a day must be considered and resolved.

References

[1] Christopher Pearce (2009), *Electronic medical records - where to from here?*. Melbourne: Professional Practice.

[2] McInnes DK, Slatman DC, Kidd MR (2011), General practitioners' use of computers for prescribing and electronic health records: results from a national survey [online], Australia. Available at: <http://www.clinfowiki.org/wiki/index.php/General_practitioners%27_use_of_computers_for_prescribing_and_electronic_health_records:_results_from_a_national_survey> [Accessed 12 September 2014]

[3] Department of Health Aging (2013), *Get your personal eHealth record now,*[online] Canberra: Department of Health Aging. Available at: <www.ehealth.gov.au> [Accessed 28 June 2013]

[4] Bosch, M., Faber, M. J., Cruijsberg, J., Voerman, G. E., Leatherman, S., Grol, R. P., Hulscher, M., andWensing, M. (2009). *Review article: Effectiveness of patient care teams and the role of clinical expertiseand coordination: A literature review*. Med. Care Res. and Rev.

[5] Kannampallil, T. G., Schauer, G. F., Cohen, T., and Patel, V. L. (2011). *Considering complexity in healthcare systems*. J.Biomed. Informatics.

[6] Malin, B., Nyemba, S., and Paulett, J. (2011), *Learning relational policies from electronic health record accesslogs*,J. Biomed. Informatics.

[7] Motta, G. H. M. B. and Furuie, S. S. *A contextual role-based access control authorization model for electronic patient record.*Information Technology in Biomedicine, IEEE Transactions on.

[8] Symantec Corporation(2006), *Strengthening Database Security*, available at: <http://www.federalnewsradio.com/pdfs/StrengtheningDataBase SecurityWP.pdf> [Accessed 30 June 2013].

[9] Barua, M., Liang, X., Lu, R., & Shen, X. (2011), *An efficient and secure patient-centric access control scheme for eHealth care system.*IEEE Conference on Computer Communications Workshops.

[10] Santos-Pereira, C., Augusto, A. B., & Cruz-Correia, R. (2013). *A secure RBAC mobile agent access control model for healthcare institutions.*IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS).

[11] Gajanayake, R., Iannella, R., &Sahama, T. (2012). *Privacy oriented access control for electronic health records.* Presented in Data Usage Management on the Web Workshop at the Worldwide Web Conference, ACM, Lyon Convention Center, Lyon, France: ACM.

[12] Ferraiolo, D.F., Kuhn, D.R., &Chandramouli, R. (2003).*Role-based access control* (2nd edition): Artech house, F.L. Bauer (2000),Decrypted Secrets, 2nd edition, Springer.

[13] Sandhu, R. S. and Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine.*

[14] Motta, G. H. M. B. and Furuie, S. S. (2003). *A contextual role-based access control authorization model for electronic patient records.*IEEE Information Technology in Biomedicine.

[15] Evered, M., &Bögeholz, S. (2004). *A case study in access control requirements for a health information system*. Proceedings of the second Australian Information Security Workshop, AISW 2004, Dunedin, New Zealand.

[16] Byun, J.-W., Bertino, E. & Li, N. (2005).*Purpose based access control of complex data for privacy protection.*Proceedings of the tenth ACM symposium on Access control models and technologies , New York, USA.

[17] Naikuo, Y., Howard, B. &Ning, Z. (2007). A purpose-based access control model.*Journal of Information Assurance and Security*.

[18] Al-Fedaghi, S. S. Beyond purpose-based privacy access control. In *Proceedings of the Proceedings of the eighteenth conference on Australasian database - Volume 63* (Ballarat, Victoria, Australia, 2007). Australian Computer Society, Inc.

[19] Amichai Schulman (2007), *Top 10 database attacks*, available at http://www.bcs.org/server.php?show=ConWebDoc.8852, U.K.

[20] NoWires Research Group, University of Bergin (July 2007), *Introduction to Database Security*, available at http://www.kjhole.com/WebSec/PDF/Database.pdf, Bergin.

[21] Tom Espiner (January 2007), *Security Threats Toolkit: Security expertscrticise government database plans*, available at http://news.zdnet.co.uk/security/0,1000000189,39285536,00.htm, U.K.

[22] Wang H., Cao J., Zhang Y. (2005), *A Flexible Payment Scheme and Its Role-Based Access Control, IEEE Transactions on Knowledge & Data Engineering,* vol.17, no. 3, pp. 425-436.

[23] Wang H., Zhang Y,Cao J. (2008), *Access control management for ubiquitous computing, Future Generation Computer Systems,* 24 (8), 870-878.

[24] Kabir E., Wang H., Bertino E. (2011), *A conditional purpose-based access control model with dynamic roles,* Expert Systems with Applications 38 (3), 1482-1489

Appendix: Implementation of the proposed model

The following sample coding has been tested to validate the system using Visual Basic.6 programming language.

```
Function checkdata() As Boolean
bcheck = True
   If txtuser.Text = "" Then
MsgBox "Enter user name", , "HighSec System"
txtuser.SetFocus
bcheck = False
       Exit Function
   End If
   If txtpassword.Text = "" Then
MsgBox "Enter Password", , "HighSec System"
txtpassword.SetFocus
bcheck = False
       Exit Function
   End If
    If cmbUsertype.Text = "Normal" Then
       If cmbManager.Text = "Select" Then
MsgBox "Select Manager", , "HighSec System"
txtpassword.SetFocus
bcheck = False
          Exit Function
       End If
    End If
checkdata = bcheck
End Function

Private Sub cmbUsertype_Click()
   If cmbUsertype.Text = "Normal" Then
       Frame1.Visible = True
   Else
       Frame1.Visible = False
   End If
End Sub
```

Coding I – New user registration

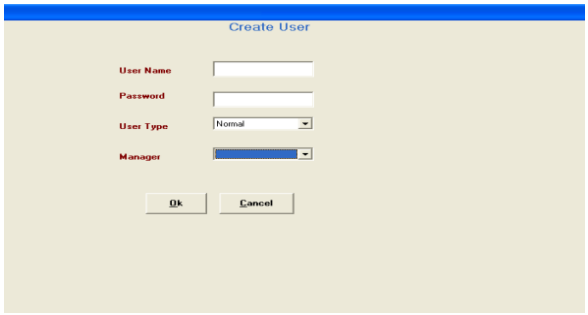


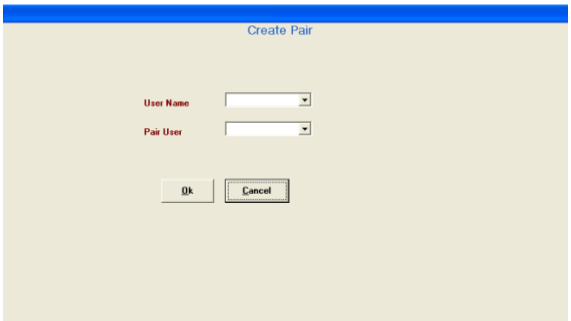
Figure 4 –System interface for new user registration

```
Private Sub cmdok_Click()
bcheck = checkdata
usertype = Left(cmbUsertype.Text, 1)
 If bcheck = checkdata Then
rs.Open "select * from usertable where userid='"
+ txtuser.Text + "'", cn
       If Not rs.EOF And Not rs.BOFThen
MsgBox "This user already exists", , "HighSec
System"
       Else
newpwd = encryptdata(txtpassword.Text,
newkey)
newpwd = txtpassword.Text
ssql = "insert into usertable (userid,pwd,usertype)
values('" + txtuser.Text + "','" + newpwd + "','" +
usertype + "')"
InputBox "", ,ssql

cn.Executessql
          If usertype = "N" Then
ssql = "insert into groupuser (user1,user2)
values('" + txtuser.Text + "','" +
cmbManager.Text + "')"
cn.Executessql
          End If
ans = MsgBox("User created succesfully. " +
vbCrLf + " Do you want to close this window?",
vbYesNo)
          If ans = vbYes Then
             Unload Me
          Else
txtuser.Text = ""
txtpassword.Text = ""
          End If
       End If
rs.Close
   End If
End Sub


Private Sub Form_Load()
ssql = "select * from usertable where
usertype='M'"
rs.Openssql, cn
While Notrs.EOF
cmbManager.AddItemrs(0)
rs.MoveNext
Wend
rs.Close
cmbUsertype.ListIndex = 0
End Sub
```

Coding II – Creating super (pair) user and the verification process



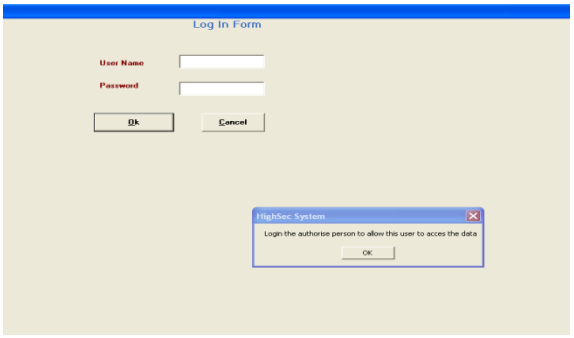


Figure 5 and 6 – System interfaces for creating new user and the verification process