MEDINFO 2013
C.U. Lehmann et al. (Eds.)

doi:10.3233/978-1-61499-289-9-812

Information Security Requirements in Patient-Centred Healthcare Support Systems

Shada Alsalamah[a,b], W. Alex Gray[a], Jeremy Hilton[c], Hessah Alsalamah[b]

[a] *School of Computer Science & Informatics, Cardiff University, Cardiff, UK*
[b] *College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia*
[c] *Department of Informatics & Systems Engineering, Cranfield University, Shrivenham, UK*

Abstract

Enabling Patient-Centred (PC) care in modern healthcare requires the flow of medical information with the patient between different healthcare providers as they follow the patient's treatment plan. However, PC care threatens the stability of the balance of information security in the support systems since legacy systems fall short of attaining a security balance when sharing their information due to compromises made between its availability, integrity, and confidentiality. Results show that the main reason for this is that information security implementation in discrete legacy systems focused mainly on information confidentiality and integrity leaving availability a challenge in collaboration. Through an empirical study using domain analysis, observations, and interviews, this paper identifies a need for six information security requirements in legacy systems to cope with this situation in order to attain the security balance in systems supporting PC care implementation in modern healthcare.

Keywords:

Clinical informatics, Patient-centred healthcare, Access control, Information security requirements.

Introduction

Information security implementation in information systems requires the three information security goals to be addressed: availability, integrity, and confidentiality must be in the right balance for an application [1]. Information should be available only to those authorised to see it at appropriate times, can only be changed by those authorised to modify it, and kept from unauthorised disclosure [1, 2]. Since information security cannot be absolute [3], the act of balancing these three goals is a key challenge in building secure systems especially as they often conflict [1, 29] (e.g., preserving confidentiality through access prevention compromises availability, this can result in an insecure system [1]). Therefore, establishing a balance that satisfies the user and the security professional is a trade-off between these three goals [3]. In traditional discrete systems, attaining this balance is achieved by creating a policy (consisting of a set of information security rules implemented using security controls) to be enforced within the boundaries of the organisational domain, which gives it a single control point with a well-understood enforcement model [4]. These security rules define a user's access rights to information resources which provides a balanced information security system meeting the business needs [5]. However, attaining the balance of information security in collaborative environments (where distributed information resources are shared among geographically and administratively distributed physical organisations [4, 6-9]) is difficult because there are multiple policy-enforcement points in different organisations with inconsistent security rules [7], which makes compliance with such policies complicated [4]. This form of collaboration is needed in modern healthcare, particularly to support Patient-Centred (PC) care. Therefore, integration of the multiple points of control in harmony is an important information security issue in modern healthcare collaborative environments. This paper discusses security in current legacy systems, and the issues faced in adopting PC care. It also identifies the information security requirements needed to maintain the stability of the information security balance at the PC healthcare level.

Patient-centred care adoption in modern healthcare

Modern integrated healthcare services are an essential part of e-health [10]. They use ICT to enhance collaboration, communication, and coordination in the health sector [8, 10]. Care integration essential to PC care [11], is defined in [12] as:

> 'A collaborative effort… where patients and the health care professionals collaborate as a team, share knowledge and work toward the common goals of optimum healing and recovery.'

In the global adoption of PC care [13-15], patient treatment is shifting from a traditional [16] fragmented disease-centred approach towards an integrated PC one [11, 14-15, 17]. PC care has a more holistic view as it considers the patient's condition as a whole [17-18], where the patient is at the heart of these healthcare services and care is integrated and tailored around the patient's needs and current state [11, 14, 19-20]. It encourages healthcare professionals to adapt to these needs [20] by collaborating as a Care Team (CT) [17] and using shared decision-making processes in regular Multi-Disciplinary Team (MDT) reviews [15]. Also each CT member collects relevant information and shares it with other members to collectively form a complete patient record about the patient's holistic condition. These treatment delivery approaches have different attributes, the key emphasis in traditional disease-centered care is on record keeping [19] while the PC approach creates a "culture of open information" [20] emphasising accessibility to patient information [19], teamwork and collaboration [17], and shared decision-making [15, 20]. PC treatment is "shared care" of a patient [16].

Methods

Domain analysis [21]**-** was conducted to understand the complexity of PC healthcare and develop a conceptual model. It is

best investigated through a real-life treatment pathway. To study the various complexities due to different treatment pathways (called integrated care pathways), breast, Upper Gastrointestinal (UGI), and Hepatocellular (HC) cancer treatment pathways were analyzed (as published in the Map of Medicine clinical guidelines [22]). PC care was studied along each of these treatment pathways and a conceptual model developed for each pathway to show different aspects of PC care. Some results from the domain analysis and part of the breast cancer conceptual model are discussed in [23].

Observation of current practice- The use of Canisc {Cancer Network Information System Cymru (the support system providing information to health professionals treating Welsh cancer patients) [24]}, Centricity {the radiology system at Velindre National Health Service (NHS) Trust}, and the Welsh clinical portal [25] was studied. The role of MDT is an essential step towards PC care [26]. It is fundamental in most treatment pathways and is a major information sharing point for care management plans. A total of six different MDT review sessions in the selected cancers pathways were observed.

Semi-structured interviews- were conducted with 10 interviewees chosen because of their knowledge of the treatment pathways used in cancer care [26]. The interviews covered how PC care was being supported from the interviewees' perspective by the current procedures linking the legacy systems and what would improve this support.

Results

The development of conceptual models helped gain an understanding of how treatment should be achieved in a PC manner. This assisted in identification of weaknesses in legacy systems, when used in implementing PC care. These issues were investigated in finer detail in the interviews, which led to the identified requirements. The issues were synthesised from the interview transcriptions [26] are presented here:

Issues in legacy healthcare systems in care management

In Wales a typical scenario is a patient visits a GP, say in Swansea, with alarming symptoms, and gets referred urgently to a gastroenterologist for oesophageal cancer diagnosis. Diagnostic tests are discussed and recorded at a local MDT review. If the patient is found fit for further potentially curative treatment s/he may be referred to Cardiff cancer service for further staging tests prior to a fuller MDT review to discuss a final management plan. The patient will receive oncology treatment at Velindre NHS Trust, while surgery treatment will be in Cardiff and Vale University Local Health Board. Both treatments are discussed at further MDT reviews. If s/he relapses then palliative care may occur locally in another NHS Trust [26]. This treatment scenario shows the distribution of care between Cardiff and Swansea with up to seven healthcare providers involved. Thus, the balance of information security must ensure that at the point of care, all CT members treating the patient are given speedy access to all the information needed for the patient's care regardless of the location, while limiting access to the absolute minimum for people not treating the patient, without affecting its integrity [26]. However, legacy support systems used in current patient case management usually fall short of attaining and retaining the stability of balance of information security for the following reasons:

Information integrity- is sometimes hard to preserve once a human error has occurred in recording information following a referred patient between different healthcare providers. If an oncologist at one organisation receives an incorrect code for the diagnosed cancer type (i.e., a code referring to a different cancer type) current systems do not allow this consultant to change it [26]. This is because the information owner who recorded it works for a different healthcare provider, and edit access is not granted to external users [26]. A major weakness in the current system is that it cannot track back to the owner and the point where the information was compiled. Even if it can, there is a need to contact the originator (if known) to request an alteration which can only be done locally in the current system [26].

Information availability- is extremely critical in patient care management, since more harm is done to the patient through lack of access to relevant information, as it prevents informed clinical decisions using it, than by misuse due to the risk of information falling into the wrong hands [26]. However, PC care compromises the availability of patient information for a number of reasons. Firstly, many legacy systems in the UK were designed in 1948 when the NHS was established [14] to meet the requirements of a disease-centric approach. All these systems adopted the NHS national high-level policies and practice guidelines, and each system adapted the policies and guidelines to meet local needs [27]. This was achieved by interpreting high-level policies into lower-level ones, resulting in different inconsistent information security policies and rules. Once information is shared, different healthcare providers can have varied interpretations of the guidance about information security rules protecting information [26]. These different interpretations may block CT members from accessing required information at the point of care [26], and current systems cannot override access permissions locally to allow access in such cases, so CT members must contact the originator to ask for relaxation of security rules [26]. This affects the treatment continuity, causes delays, and limits the collaboration's effectiveness. Secondly, the big challenge in information security solutions in healthcare systems is that life threatening emergency situations require resilience, most importantly when the patient is unconscious and decisions mean life or death [26]. In such cases, there is a need to access any information stored about the patient at very short notice. This may require trusted CT members to access information not normally required for their role [26] and, this means a need to enable immediate access by forcing the system to yield to CT access needs and relax already assigned access rights when every second counts, then restore these levels of information security after the emergency event to give systems the resilience needed in such cases. This introduces the need for a "circle of trust" implementation (explained later). A major weakness in current legacy systems is the lack of a way to deal with such cases [26], when writing to the original organisation requesting access, may delay or prevent the treatment happening in a timely fashion [26].

Moreover, to help track patient treatment as a single business process, systems supporting healthcare should reflect the care management occurring in a number of healthcare organisations, and the flow of their information following the treatment pathway [26]. Currently, enhanced legacy systems supporting PC healthcare are designed to organize patient case-note data in parallel on a healthcare-provider basis and not in sequence on a treatment-point basis [26]. Thus information management is based on the healthcare provider and each patient's case-notes are split into parallel partitions where each provider

holds relevant information for a disease or part of the treatment in their partition [26]. Each provider owns and controls their part of the information, and they give direct access to it by listing CT member's names as having access [26]. If a CT member happens not to be listed for access to the information (normally caused by the interpretation of security rules), he will have no access until the other provider grants it [26]. This structure sometimes makes it difficult to find relevant clinical information and causes information duplication in the partitions [26]. This can cause inconsistency issues directly affecting the patient's clinical care. Also, problems can lead to losing track of patients and their information at some point in the treatment pathway. For example, it may be unclear which CT member is responsible for the patient's follow-up after treatment leading to the patient not receiving a necessary service [23, 27]; or care management may be interrupted when information does not flow with the patient from one provider to another on the clinical pathway (e.g., when patients are referred to Cardiff from Swansea but scan images do not follow, this can make critical information unavailable at a treatment point and cause incorrect treatment) [26].

Information confidentiality- is essential due to movement towards a culture of open information, in which information access is a priority to healthcare professionals [15, 20]. A higher degree of information sharing is needed in PC care than in a traditional approach [8, 15]. Confidentiality can be breached in PC care if information is improperly disclosed to unauthorized people. Two factors increase the risk of improper disclosure of information: the number of people having legitimate access to the information, and the value of this information [28]. The higher risk of disclosure to unauthorized people is due to the NHS planning to integrate all relevant systems of 100 Health Authorities, around 3,500 GPs and over 400 NHS Trusts, in the modernisation of UK healthcare systems [14]. Also, there is a direct correlation between valuable information and the risk of its disclosure [28]. There are many reasons why systems supporting healthcare store highly valuable information. First and foremost, clinical information has value as a basis for healthcare professionals' decision-making processes, and its corruption can lead to incorrect decisions, which may harm or even kill a patient [28]. The systems hold extensive patient information, which may contain personal, embarrassing, and critical medical information [23]. This information has a longevity characteristic [29], meaning it is highly sensitive [16] and confidential [26, 30] at all times. Therefore, its nature means medical information should only be disclosed for permitted medical purposes [30]. This puts PC information at great risk of improper disclosure [28] and stresses the need to protect information from those not needing it, while ensuring availability of life-critical patient information on a need-to-know basis at the time of care [30].Finally, according to Pfleeger [1] "centralized control of access is fundamental to preserving confidentiality and integrity, but it is not clear that a single access control point can enforce availability." This is clear from the discussion above where most of the information issues are about availability. This is expected as much of the research reported in the literature has focused on confidentiality and integrity, and full implementation of availability is security's next great challenges [1]. This means that information security implementation in legacy discrete systems supporting the traditional treatment approach mainly focused on the confidentiality and integrity of medical information as they were an issue while availability was not. Thus, the key reason why they fall short of attaining a security balance in PC care is that information availability only became an issue with collaboration.

Information security requirements

For legacy systems to address these issues in PC care, they need to deal with six key information security requirements:

Role-base access control- Access to medical information must be on a need-to-know basis [30]. Thus before sharing medical information, information owners must guarantee granular access to the information based on a healthcare professional's role in the patient's treatment.

Fine-grained access control- Different roles have different information-access needs, and privacy violations can be expected if all members in the healthcare environment can see every patient's records [28]. Also although clinical information is confidential [26, 30], it has different levels of sensitivity [26]. Examples include systems recording details about social services, HIV positive results, and paediatrics systems recording child abuse information [26]. This information can be labelled as being more sensitive. Thus it is key to have fine-grained access control that enforces security rules within a resource at different granularity levels [9] by moving information security controls from a coarse-grained to a finer-grained level [9]. This will give legacy systems the flexibility to provide different protection levels for different parts of the information resource based on sensitivity level, and thus, enable resilience. When an information resource is shared in its entirety, different parts of the information will be accessed by authorised people based on their sensitivity level [9]. This will need an information classification scheme based on granularity classified according to its sensitivity levels. Granular access to certain parts of the information should correspond to a healthcare professional's roles in the patient's treatment. Thus, access privileges are assigned to a role instead of a user, and users are assigned to roles.

Circle of trust- as well as the above access controls, which balance the fine line between availability and confidentiality of information, there is a need for a mechanism to differentiate between authorised users who need immediate access to information in emergency (the CT members trusted to break the glass) and other authorised roles that do not [16] by using the circle of trust. This circle stretches across the security domains of all collaborating health providers to include all CT members treating the patient no matter where they work.

Persistent control- the longevity characteristic of medical information means its value may never decay, and thus even archived records relating to deceased patients may remain confidential. It is therefore critical in PC care to have constant protection with information security controls that move with the information. This assures that information will only be disclosed to people using it for permitted medical purposes regardless of its location in the treatment pathway [30]. Enabling such persistent control requires an ability to track the flow of information among its authorised users as it crosses the boundary of the organisational protection system. This should be sequentially organised to facilitate its tracking.

Dynamic control- is also needed to provide information owners with full control over their information by being able to change the level of protection and even update the information remotely at any time after the information is shared and stored in systems outside their organisational boundary. Changing protection level is key when legacy systems do not follow guidelines and blocks legitimate users, while being able to alter information will assist in retaining its integrity in case of a disastrous error.

Human-level policy awareness- a well-designed system must take people into account [31] because as Pipkin [2] states "most of an organisation's intellectual property is contained in the minds of the organisation's employees." Based on a firm belief that the protection of patient information is a cooperative responsibility of all the healthcare professionals involved, and because shared care cannot be achieved without healthcare professionals thinking patient-centrically, this paper suggests raising awareness around PC care and information security needs to be addressed at two different levels: at the collaboration level by running information security awareness training for staff of all providers; at the human level, the system provides simple and readable policies which are attached to protected information to inform a user of its protection level classified by the owner.

Realizing requirements in patient-centric implementation

In this section, the implementation of the requirements to address the categorised information security issues is discussed.

Information integrity issue- can be addressed in two ways. First, by tracking the information flow against the treatment points; this helps identify a CT member who recorded information incorrectly and the owner. Second, the system should enable the owners to correct such information remotely from a system in another organisation. This requires the provision of persistent and dynamic control over information.

Information availability issues- can be addressed by using persistent and dynamic controls. Thus, when CT members are blocked from accessing information, the system allows information owners to relax security rules remotely and when members of the circle of trust need speedy access to override any rules blocking it. This needs extra support in current systems to easily track and give access to information based on the sequence of treatment points and time. This will make it easier for CT members to find relevant information about the patient and not lose track of the patient and their information. Also varied interpretations of policies can be avoided by raising human awareness at the PC care level. This requires educating healthcare professionals about PC care and attaining a security balance in shared care. This training is essential in understanding the policies of other providers showing how hosting system should protect their information. Also, communicating these policies with the information in a readable manner ensures a high level of awareness among all CT members. The other availability issue is addressed by having a 'breaking-glass' feature in emergency cases. This preserves patient privacy when confidentiality is needed, while providing the required resilience to deal with emergency cases. The concept of a glass box is to store information with a high level of sensitivity, means it is kept behind the glass and protected using tighter security rules and controls. Thus it is more secure and protected, while the resource is available for sharing with those in critical need of it. The usage of this feature is expected among CT members, and therefore they are added to the circle of trust for distinction with a supporting alarm system in place to report any breach of trust happening when someone outside the circle of trust tries to break into this sensitive information. This feature is achieved at two levels; before and after an incident. First, the system should support fine-grained access control, with information classified according to its sensitivity level. Then each category is assigned a set of security rules and controls reflecting the required protection level to give the system the flexibility needed while protecting patient privacy. After a glass is broken, the system should recover by restoring the required levels of security balance, and requesting a justification. Access monitoring and audit analysis is needed at all times to identify the user accessing the information and to react in a case of privacy invasion. Studying these incidents assists in learning more about how to adapt systems to meet future needs.

Information confidentiality issue- cannot be solved without consideration of availability issues discussed above as these requirements are in direct conflict [1, 29], which makes it hard to achieve a balance with current computer security mechanisms [32]. Therefore, to attain the balance between availability and confidentiality, the circle of trust is used to distinguish CT members from other authorised users. After properly authenticating a user, the system should be able to make decisions that control information access based on the user's role and being in the circle of trust. This relaxes security rules applying to users in the circle if immediate access is needed, but not for those outside the circle. Fine-grained control is important as it maintains the confidentiality level while giving flexibility to tighten the security rules based on the information's sensitivity level.

Discussion and conclusion

PC healthcare is significantly enhancing the quality of care, but it reveals weaknesses in current legacy healthcare support systems. There is a need to facilitate provision of adequate means for communicating information at all stages of a patient's treatment pathway, regardless of location of a treatment point. This is achievable by rebalancing the levels of information availability, integrity and confidentiality with the resilience which healthcare environments require. However, legacy systems cannot support the balance of information security when information flows between different healthcare providers as their information security implementation is focused on information confidentiality and integrity. Using a mixture of qualitative research methods has led to the identification of six key information security requirements to enable legacy systems to achieve this balance and, thus, facilitate the implementation of PC care. Results show a need for: access that is fine-grained and based on a healthcare professional's role; employing the circle of trust concept; persistent and dynamic control over this access across inter-connected systems' boundaries; and raising the information security awareness of collaborating users. However, implementation is affected by a number of factors. First, older legacy systems do not have the required facilities, while newer systems may provide some of the requirements. Second, variation in security levels of the collaborating systems means aggregating information from a healthcare provider employing a higher level of security with tighter security controls than the hosting system can be a problem and vice versa. Thus, implementation requires the selection of different information security mechanisms, and the success of the implementation will depend on this selection. The selection itself will be based on the functionality of the existing system, and the protection level required. The challenge lies in ensuring that the protection level is not reduced when information with high-level protection is moved to a system with lesser protection, and this can be resolved by breaking down the protection using its granularity. Finally, improving the effectiveness, dynamism, and potential of collaborative efforts in PC care requires extensive collaborative efforts and a major shift in organisational and cultural thinking to make it more integrated. This is almost as important as shifts in practice due to PC working.

References

[1] Pfleeger CP, and Pfleeger SL. Security in Computing. 3rd ed. New Jersey: Prentice Hall, 2003.

[2] Pipkin DL. Information Security Protecting the Global Enterprise, New Jersey: Prentice Hall, 2000.

[3] Whitman ME, and Mattord HJ. Principles of information security. Boston: Course Technology, 2012.

[4] Wasson G and Humphrey M. Policy and enforcement in virtual organizations. In Fourth International Workshop on Grid Computing. Washington DC, USA, IEEE Computer Society. 2003; pp. 125–132.

[5] Posthumus S and Von Solms R. A framework for the governance of information security. Computers & Security 2004: 23(8): 638–46.

[6] Park J, Sandhu R. Towards usage control models: beyond traditional access control. In Proceedings of the seventh ACM symposium on Access control models and technologies. New York, NY, USA: ACM, 2002; pp. 57–64.

[7] Yau S. and Chen Z. Security Policy Integration and Conflict Reconciliation for Collaborations among Organizations in Ubiquitous Computing Environments. In F. Sandnes et al., eds. Ubiquitous Intelligence and Computing. Springer Berlin Heidelberg, 2008; pp. 3–19.

[8] Eysenbach G. What is e-health? J Med Internet Research 2001: 3(2): e20.

[9] Burnap P and Hilton J. Self Protecting Data for Deperimeterised Information Sharing. In 2009 Third International Conference on Digital Society. Cancun: IEEE, 2009; pp. 65–70.

[10] Powell J. Integrating healthcare with ICT. In W. Currie and D. Finnegan, eds. Integrating Healthcare with Information and Communications Technology. Radcliffe Publishing Ltd, 2009; pp. 85-94.

[11] Allam, O.. A Holistic Analysis Approach to Facilitating Communication between General Practitioners and Cancer Care Teams. PhD Thesis. Cardiff University. Cardiff, UK: 2006.

[12] International Alliance of Patient' Organizations (IAPO), What is Patient-Centred Healthcare? A Review of Definitions and Principles, London. 2004.

[13] Ellingsen G, Røed K. The Role of Integration in Health-Based Information Infrastructures. Computer Supported Cooperative Work (CSCW) 2010: 19(6): pp.557-84.

[14] Department of Health (DoH). The new NHS: modern, dependable, London: HMSO, 1997.

[15] Skilton A. Using Team Structure to Understand and Support the Needs of Distributed Healthcare Teams. PhD Thesis. Cardiff University. Cardiff, UK, 2011.

[16] Smith E and Eloff JH. Security in health-care information systems--current trends. International journal of medical informatics 1999: 54(1):39-54.

[17] Al-Salamah H, Gray WA and Morrey D. Velindre Healthcare Integrated Care Pathway. In L. Fischer, ed. Taming the Unpredictable Real World Adaptive Case Management: Case Studies and Practical Guidance. Lighthouse Point: Future Strategies Inc., 2011; p. 227.

[18] American Cancer Society. Holistic Medicine. Available at: http://www.cancer.org/Treatment/TreatmentsandSideEffects/ComplementaryandAlternativeMedicine/MindBodyandSpirit/holistic-medicine 2008. [Accessed March 31, 2013].

[19] Dawson J, Tulu B and Horan TA. Towards Patient-Centered Care: The Role of E-Health in Enabling Patient Access to Health Information. In E. V. Wilson, ed. Patient-Centered E-Health. London: IGI Global, 2009.

[20] Department of Health (DoH). Equity and excellence: Liberating the NHS, London: HMSO, 2010.

[21] Fernandez EB, Yoshioka N, Washizaki H, Jurjens J. Using security patterns to 'build secure systems. In 1st Int. Workshop on Software Patterns and Quality (SPAQu 2007). Nagoya, 2007.

[22] Map of Medicine. Map of Medicine. Available at: http://www.mapofmedicine.com/solution/whatisthemap/ 2012. [Accessed March 31, 2013].

[23] Alsalamah S, Gray A, and Hilton J. 2011. Towards Persistent Control over Shared Information in a Collaborative Environment. In L. Armistead, ed. Proc 6th Inter Conf Information Warfare and Security (ICIW). Washington, DC: Academic Publishing International Limited, 2011; pp. 278-87.

[24] NHS Wales Informatics Service (NWIS). Canisc. Available at: http://www.wales.nhs.uk/nwis/page/52601 2013. [Accessed March 31, 2013].

[25] NHS Wales Informatics Service (NWIS). Welsh Clinical Portal. Available at: http://www.wales.nhs.uk/nwis/page/52547 2013. [Accessed March 31, 2013].

[26] Some of the 10 interviewees' job titles are: chair of the cancer service management board, head of the software service unit at the Velindre cancer centre, head of information management & technology, cancer centre Caldicott guardian, support manager, governance and security specialist, GP, breast cancer consultant clinical oncologist, breast cancer nurse specialist, UGI cancer consultant clinical oncologist, and MDT coordinators for normal breast, metastatic breast, UGI, and HC cancers.

[27] National Institute for Healthcare and Clinical Excellence (NICE). Improving Outcomes in Breast Cancer- Manual Update. 2002.

[28] Anderson RJ. Security in Clinical Information Systems. London: BMA, 1996; p.32.

[29] Beale T. 2004. The Health Record - Why is it so hard? In Haux R and Kukikowski C, eds. IMIA Yearbook of Medical Informatics 2005: Ubiquitous Health Care Systems. Stuttgart, 2004; pp. 301-04.

[30] Department of Health (DoH). Confidentiality: NHS Code of Practice, London: HMSO, 2003.

[31] Schneier B. Why Cryptography Is Harder Than It Looks. Information Security Bulletin 1997: 2 (2): 31-6.

[32] Anderson RJ. Security Engineering. 2nd ed. Indianapolis: Wiley Publishing, 2008.

Address for correspondence

Shada Alsalamah. S.A.Salamah@cs.cardiff.ac.uk.