Safety Measures for Social Computing in Wiki Learning Environment

Ahmed Patel, Universiti Kebangsaan Malaysia, Malaysia, and Kingston University, UK

Mona Taghavi, Universiti Kebangsaan Malaysia, Malaysia

Joaquim Celestino Júnior, State University of Ceará, Brazil

Rodziah Latih, Universiti Kebangsaan Malaysia, Malaysia

Abdullah Mohd Zin, Universiti Kebangsaan Malaysia, Malaysia

ABSTRACT

Wikis are social networking systems that allow users to freely intermingle at different levels of communication such as collaborative learning, chatting, and group communications. Although a great idea and goal, it's particularly vulnerable due to its features of open medium and lack of clear plan of defense. Personal data can be misused for virtual insulting, resulting in misuse of personal information for financial gains or creating misuses. Wikis are an example of social computing of collaborative learning, joint editing, brain storming, and virtual socializing, which is a ripe environment for hacking, deception, abuse, and misuse. Thus, wiki needs comprehensive security measures which include privacy, trust, security, audit, and digital forensics to protect users and system resources. This paper identifies and explores the needs of secure social computing and supporting information systems as places for interaction, data collection, and manipulation for wikis. It does this by reviewing the literature and related works in proposing a safety measure framework for a secure and trustworthy medium together with privacy, audit, and digital forensic investigative functions in wiki environments. These then can aid design and usage in social computing environments with the proviso to give comfort and confidence to users without worrying about abuse and cybercrime perpetrated activities.

Keywords: *Collaborative Learning, Safety Measure, Security, Social Computing, Wikis*

INTRODUCTION

Social Computing is a general term in Information and Communication Technology (ICT). Actually, it is concerned with the intersection of social behavior and computational information systems which is bringing more and more people into the communication cycle and patterns of activities. Social computing is one of the most popular and dynamic trends on the Web today. In fact, wikis and other activities that engage people in collective activities via the Internet

DOI: 10.4018/jisp.2012040101

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

have challenged traditional business models, created new ecosystems of content and people, and fundamentally transformed the way people manage their professional and personal relationships (Aronsson, 2002). Recently, venture capital investments have focused around enterprise social computing solutions at an increasing rate (Newsgator, 2009). Wiki as a social computing application trend is an appropriate useful and very helpful platform that enables online collaboration and creation of a knowledge based society. Wiki can be accessed and amended by anyone on the World Wide Web through the Internet. Wikis leverage the experience and knowledge community participants by giving individuals the ability to tag the profiles of others, or rate their participation in forums or their responses to questions. These approaches allow users to build reputation scores as well as publicize their areas of expertise to other participants (Lazar, 2010). Communities and sharing of personal information may raise concerns about privacy. It indicates that users' trust in other community members, and the community's information sharing norms have a negative impact on community-specific privacy concerns. Assessing information risk from the start, do not discount regulatory issues, and ensure information security and protection permeates at every step. Balance carefully the benefits of openness versus locking down the environment. Therefore, this paper focuses on identifying and exploring the needs of secure social computing and supporting information systems as places for interaction, data collection and manipulation with more emphasis on wikis in education context.

This paper is organized as follow: First, we briefly outlines the principles of social computing and wiki. Then we explain wiki safety measures. The *Collaborative Learning Environments* using wiki is described and we then present the review of social computing challenges. Following that we give detailed description of social computing safety approaches which include security, privacy, trust, audit and digital forensics. Finally, a discussion is given and an overall conclusion is discussed.

PRINCIPLES OF SOCIAL COMPUTING

The focus of social computing is the possibility of designing digital systems that support the users by making their socially produced information available to all users. In order to enhance the functioning of a system, it uses the information that is produced by a group of people. Social computing should address certain issues as security, privacy, trust and risk to support a secure and trustworthy trading environment (Motahari et al., 2007). Social computing can be defined as any type of computing application in which software serves as an intermediary or a focus for a social relation (Schuler, 1994). It also refers to systems distributed across social collectivity which gather, process, represent, use, and disseminate the information. Moreover, the information is significantly precise since it is associated with people, who are linked to others. Also a social structure in which technology puts power in communities individuals and not institutions (Charron et al., 2006). Finally computational facilitation of human social dynamics and social studies as well as the design and use of ICTs that consider social context (Wang, 2005).

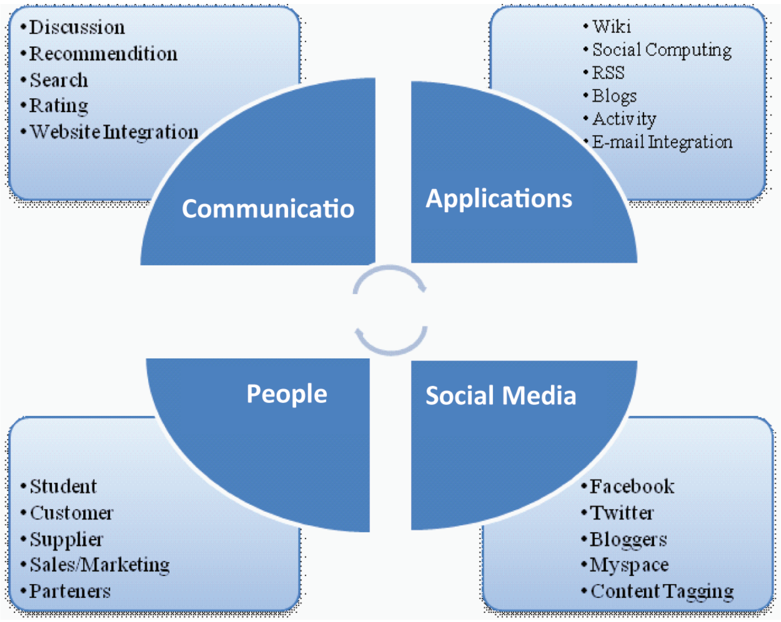
While wiki can be defined as Web-based software, it allows easy creation and editing of any number of interlinked pages by the site viewers via a web browser using a simplified markup language or *What You See is What You Get* (WYSIWYG) text editor. In fact, wikis are typically powered by wiki software and are mainly used to create collaborative wiki websites, to power community websites, for personal note taking, organization intranets, and in knowledge management systems (Thite, 1999).

A Wiki is simply a set of linked Web pages and applications enabling its development, created through the incremental linking of such pages by a group of collaborating users. The Wiki is unique by both in its software and in the use of the software by collaborating members.

Wikis site is an example of how social technology facilitates collective participation

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 1. Social computing tools



and creates new forms of social expression. Wiki is moving beyond the public domain to permeate the workplace. Figure 1 shows the content of social computing tools in terms of applications, social media, methods of communication, and target set of users.

As shown in Figure 1, MySpace, Twitter, or Facebook typically provide applications for people/users to set up individual profiles to create virtual networks by communicating with friends, mates and partners. Actually, they share articles, videos and photos, create content such as stories and blog entries, or to share opinions or preferences. Increasing online collaboration, interaction and personalization is the result – something that online advertiser's value as the source for more targeted marketing initiatives using sophisticated data mining capabilities. Wiki in a classroom is one example of online collaborative tool which provides applications for users to set up individual profiles to create virtual networks with students, share articles and projects.

SAFETY MEASURE ISSUES IN WIKI WEB SITES

Lars Aronsson indicated that a data system specialist summarizes this debate as follow: "Most of the people, when they first learn about the wiki concept, assume that a website editable by anybody would soon be rendered useless by destructive input. It seems like offering free spray cans next to a grey concrete wall. The only likely consequence would be ugly graffiti and simple tagging, and many artistic efforts would not be long lived. Still, it seems to work very well" (Aronsson, 2002). Several reviewers of open-source wiki systems have stressed that these systems could be easily tampered with and sometimes even vandalized. That is, allowing anyone to edit wiki content does not ensure by any means that all contributors have virtuous intentions. On the other hand, wiki supporters argue that the communities of legitimate users are able to detect malicious or offensive content and correct it.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

To some extent, social computing poses the risk of a new digital divide as new applications and technologies cobble together. A lack of critical analysis, skills and awareness of the nature and the quality of the wiki contents may cause the users or the viewers not to question the accuracy and reliability of the information. For instance, patients who are using wiki could use peer support collaborative dialogue for self-diagnosis, or citizens could be misled by political or commercial opinions though devious information manipulation. These are complex issues requiring a suitable set of safety measures.

There are valid reasons for protecting a wiki. One of the most common concerns of wiki users is the security of their pages and how the page could be protected without being purposely manipulated either during development or run time. Given the "open source" nature of wiki, this is regarded as a significant threat. Other major threats relate to information security of wiki sites, information safety and its privacy. In general, all the social networking issues about impersonation and identity theft, cyber stalking, bullying and grooming create new threats for students in wiki classroom. Above all, obscurant data ownership and lack of user's control of their owned data are generating novel privacy invasion schemes producing new risks. Therefore, safety measures are essential to cover all aspects of social networking like wiki.

Apart from wiki content abuse, known sometimes as trolling, vandalism can be a major problem. Especially in large and active wiki sites with rapid changes, vandalism may not be detected even after a period of time which decreases user's trust. Presently, most wikis handle vandalism by limiting the damage through rollback (re-do) actions rather than attempting to proactively prevent damage (Jensen, 2009). In future, it might be necessary for wiki sites to deploy advanced mechanisms for audit and digital forensics, like *bots* which automatically identify cyber vandalism. This can be done by tracking how many characters have been added in each edit operation. Using these countermeasures, the treats of cybercrime and misdemeanors can be greatly contained and reduced.

As illustrated in Figure 2, social computing needs a combination of safety measures to provide a comprehensive and effective solution. Figure 2 shows the safety measures of wiki environment by considering security, trust, privacy, audit and digital forensics in wiki engine content.

SOCIAL COMPUTING AS A COLLABORATIVE LEARNING ENVIRONMENT USING WIKI

Social computing is a set of open source web-based applications which enables Internet users to share data, networking, collaborating and co-producing contents. Additionally, it includes applications such as: collaborative websites where users can share and create new content such as in *Wikipedia*.

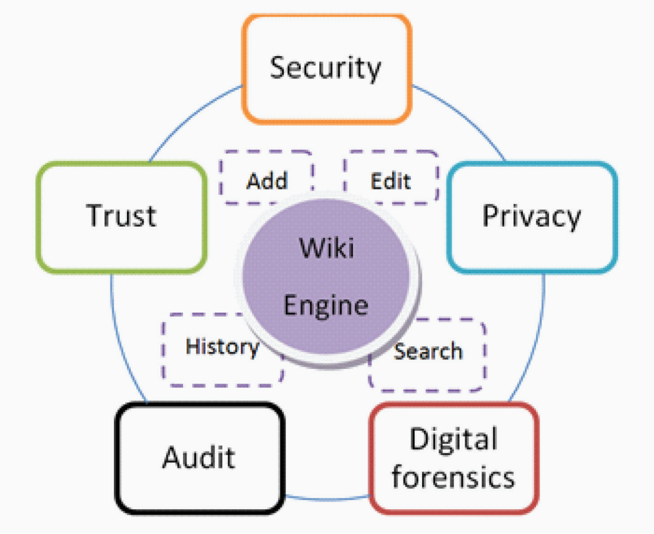
Due to the involvement of social computing in several recent trends include growing popularity of Web 2.0 and social software, the increase of open source as a feasible method of production, attracting academic interest to social network analysis, and a growing conviction, it has become more widely known and used (Li et al., 2008). Figure 3 illustrates the management framework of social computing with 3 layers of application, technological infrastructure, and theoretical underpinning.

Social experiences and interactions can be critical to conceptualization and design of the environment and may actually serve as a better starting point in the design and implementation of standards. Information privacy and collaborative environments related concepts are identified as priority research fields (Clarke, 2001). Collaborative environments not only need to protect privacy, but they must also effectively manage personal data transmitted in to, within, and out of the collaboration.

On the other hand, security risks arise from the fact that a user seems to deal more confidently with other people in virtual space. In this case, the user is required to adhere to

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 2. Social computing safety measure features



the instructions mentioned below. In fact, social computing applications have weak user identification management systems since most systems require an email ID/username and password identification. It reduces the reliability of the identification and makes it easier to hack into someone's account. Moreover, user-contributed content can be damaged via various forms of malicious software.

Accordingly, any wiki's user will need the following basic instruction to be safe online:

1. Users may share their interests, ideas and preferences, but must not disclose any personal information.
2. Users must not share username or password or even log in as others' account.
3. Deal with wiki as virtual classroom space and never use speech that is inappropriate "in polite speech during the wiki class" for wiki class.

Social computing provides a theoretical context for investigating the ways in which the environment can create rich social experiences that serve as a foundation for building effective learning support. Social computing refers to using information systems as places for social interaction as well as spaces for data collection and manipulation. Social computing occurs as awareness, communication and collaboration in virtual places, and is organized by time, object affinity and proximity.

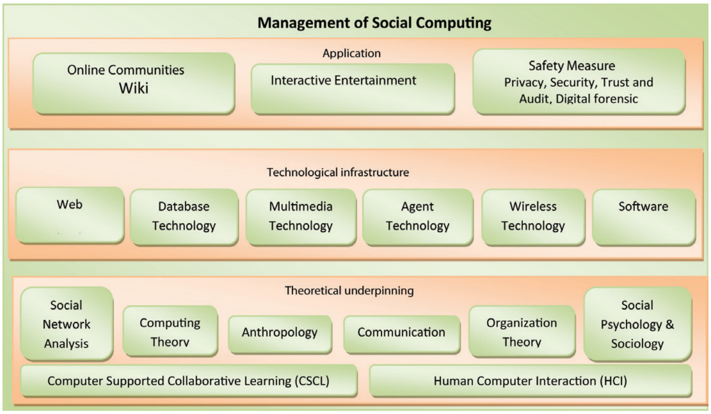
A social computing and collaboration architecture must include specifications and high level application development support for the following kinds of construct and capabilities (Musser et al., 2003):

- Representation of user presence and action.
- Representation of place.
- Formation and representation of groups.
- Social rules management.
- Communication.
- Collaboration facilities.
- Notification.
- Ubiquitous access.
- Human-Computer Interaction (HCI) elements.
- Learning environment constructs.

As a result, the education system can be developed around the concept of 'Learning spaces'; open and creative social spaces which

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 3. The three layer framework of social computing


Management of Social Computing
Application
Online Communities
Wiki
Interactive Entertainment
Safety Measure
Privacy, Security, Trust and Audit, Digital forensic
Technological infrastructure
Web
Database Technology
Multimedia Technology
Agent Technology
Wireless Technology
Software
Theoretical underpinning
Social Network Analysis
Computing Theory
Anthropology
Communication
Organization Theory
Social Psychology & Sociology
Computer Supported Collaborative Learning (CSCL)
Human Computer Interaction (HCI)

connect formal and informal learning and communities of practice as well as to allow individuals to learn according to their preferences, interests, time and skills. While guidance and interaction will continue to be crucial, the role of teachers, tutors and trainers can change as a result of social computing mechanisms, safety and rules, which will make reputation and feedback more important than official roles and titles. Table 1 compares Wiki, Blog, and Forum as three important social computing applications and shows high capabilities of wiki to serve as a learning environment. Nonetheless, employing wiki regardless of the safety issues imposes a high risk and can cause serious problem since wiki has a higher risk in comparison with other applications.

THE SOCIAL COMPUTING EVOLUTION

Social computing could address many challenges, such as helping students to find relevant information and expertise more quickly; increasing interactive collaboration across the enterprise, breaking down silos; spurring radical innovation; attracting and retaining students; and capturing the tacit knowledge of existing students. Additionally, if ICT does not provide a social computing platform, use of fragmented internal tools and insecure external tools will continue to grow.

The social computing described above must be integrated with learning environment architecture to enable social computing in education. Learning technology architectures and learning design specifications take a benign stance toward social context. The new world of social computing changes the focus to:

- People - understanding preferences from relationships and communication versus data and objects.
- Collaboration - contribution of knowledge and sharing of ideas in a creative environment versus workflow and control.
- Content-as-a-Service - content accessible everywhere, shared drive and repository. Facebook with automatic and appropriate storage, management, security, auditing and retention versus a content suite and user driven storage.
- Context of Networks - activity driven context based on content, projects and team versus person only.
- People-Centric Tools - the office versus interfaces and systems.

Wiki trend incorporated the following capabilities into the social computing platform:

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Table 1. Comparing the three social computing applications

Category	Wiki	Blog	Forum
Communication Support			
Student-instructor and student-student interaction.	It is essentially a peer feedback system without formal distinction between instructor and student input, since the paradigm upon the Wiki is based on modifying or expanding the work of others.	There is no formal distinction within the system between the student and teacher communication interaction as the paradigm is based upon *a personal journal* model.	Interaction is based upon a posting to the forum and expected reply process.
Types of media supported	Since the Wiki is based on open source and web-based software, the artefacts developed in a Wiki are web pages which can support any media types that can be displayed on the Web.	Since the blog is based on open source, web-based software, the journal postings are Web pages. This allows any media types to be displayed on the Web.	Forum largely limited to written text with the option to attach files containing audio, video, and graphic media to postings.
"Openness" of the environment	Fundamentally an open environment available to all participants through Web access.	Fundamentally an open forum available to all actors through Web access.	Typically a closed system with limited users which is available only to registered members.
Delivery modality	Basically a "pull" system, which requires users to regularly access it to determine the new changes.	"Push" system that actively prompts users through syndication to participate.	Essentially "pull" requiring members to access the forum to find out whether new postings are available.
Process Structure			
Locus of control	Principally democratic as all users can manipulate the work of others freely.	Individual author is the owner of each blog.	Instructor.
Organizational paradigm	Prototyping system with evolving web pages.	Electronic journal in the form of a diary.	Reply structure.
Information Process			
Support for student-content interaction	Students become co-creators of content.	Individual student becomes the creator of content.	Despite of offering unlimited potential for considerable depth and breadth of postings to forum, there is no specific *structure* to promote such activity that results in a great number of rather shallow and "social filler" postings.
Tools for artefact development	Simple tool set for developing Web pages.	Simple tool set for developing Web pages.	None native, beyond basic HTML tags.
Nature of the artefact developed	Web site.	Electronic journal containing authors' thoughts and comments from readers.	Textual. Lacking system- provided structure to support and maintain orderly interaction.
Features			
Posting/ Edit content	Anyone can edit or add content easily without any intervention from the administrator.	Usually done by the blog owner. Visitors can post comments to a particular posting, but it requires approval from the blog owner before it becomes available on the site.	Any registered member can post a message but in general you might need approval of the administrator to avoid masquerades and misrepresentations. Visitors or other users can reply to the message, but cannot change the original post.
Contributing	In a Wiki environment everyone is contributing. He /she can edit anyone's content, and even complete the uncompleted content. It lacks control.	The blog owner writes (creates) the content and other readers can comment upon it. So the blog owner is the main contributor.	For a particular topic, the participants are the contributors to the topic, but only the administrator can change the core topic content.

continued on the following page

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Table 1. Continued

Safety Measure			
Security	Security of content is guaranteed because almost anyone can edit or add content freely without any intervention from the administrator.	Good level of content security provided because posting is done by the blog owner. It requires approval from the blog owner before showing it on the site.	Good level of content security because any registered member can post a message but in general you might need approval of the administrator for that.
Privacy	Privacy is not protected or guaranteed because in a Wiki everyone is contributing.	Good privacy, the blog owner is the main contributor, thus can provide the necessary protection through identity management tools.	Very good privacy, only the administrator can change the core topic content through anonymity and shielding initiator.
Trust	Critics of publicly editable Wiki systems argue that these systems could be easily tampered with, while proponents argue that the community of users can catch malicious content and correct it. This is still a contentious problem.	The blog owner manages adding post therefore, the comment can be trusted.	The administrator can add, change or delete content. The information can be trusted because specific persons are responsible. The administrator is ultimately held responsible.
Audit	Not supported	Not supported	Not supported
Digital Forensic	Not supported	Not supported	Not supported
Risk	There is a risk	Not much risk	Not much risk

- Social Collaboration - knowledge spaces, calendars, discussions, wikis, social tagging, and richer social networking information for users.
- Choice - no tie-in to specific operating system, application server, portal, database, collaboration and social networking tools.
- Rapid Innovation - easy to mash up and integrate using lightweight scripting, REST style interfaces and Flex.
- Integration of External & Internal - combine both internal and external contents, services and networks seamlessly through user-driven interfaces.
- Best-of-breed and Open Source - allows mixing of industry lead Open Source tools and applications with Open Source packaging and distribution, with no vendor lock-in.

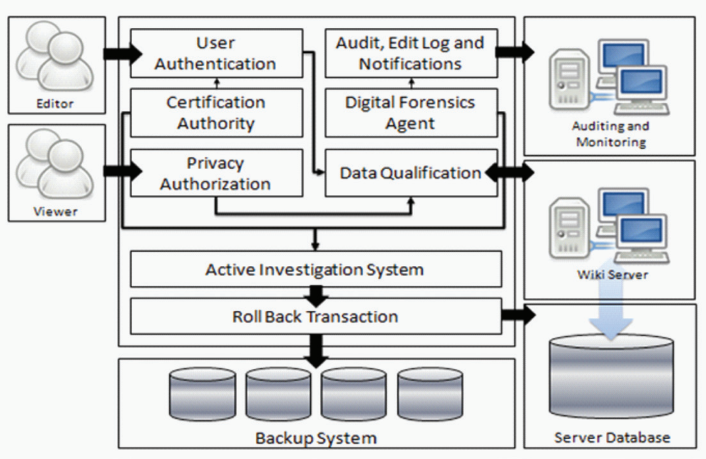
SAFETY MEASURE FRAMEWORK FOR WIKI

In fact, social computing begins with observing the sociable characteristic of humans in natural. During the time that humans grow up, they develop their interacting abilities with each other ranging from expression and body language, with written and spoken language. Therefore, people are sensitive to the behavior of those who interact with, and make numerous decisions that are affected by their social context. Upon conversation when, for example the audience starts choosing the crowded restaurant over the nearly empty one, or buying a product because everyone else is doing so, social information provides a basis for planning, inferences and coordinating activity.

The management framework was created to formalize a reference model that identifies common functions across these safety measures. It sets forth the building blocks required to achieve social computing safety management in wiki as safety measures architecture illustrated in Figure 4. Safety measures are very important to make humans communicate freely without undue complicated measures or over imposing restrictions in an open social networking environment. Table 2 illustrates applicable safety measures for wiki.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 4. Safety measures architecture



Security

As people increasingly depend on the information stored in open collaborative authoring systems, security is becoming an important concern for such systems. Improving the completeness, correctness and integrity of information in collaboratively authored documents are therefore of vital importance for continuous successful running of such systems (Jensen, 2009). Host computers and infrastructures should be trusted, need to be protected from abuse, secure from threats, safe to use, protect the user and provide privacy if necessary, and above all, be identifiable and audit- able. All these different aspects coming together as requirements which are essential for a secure, trusted and safe mobile agent-base e-business environment to operate successfully (Borselius, 2002).

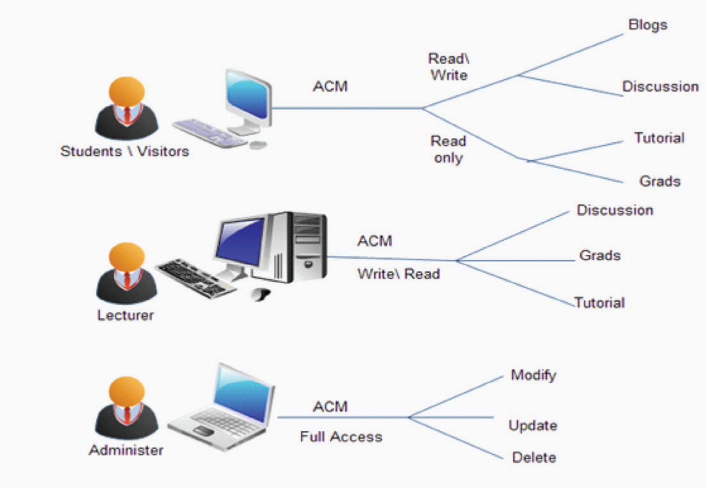
Security at the application level covers many aspects including authorization, authentication, message integrity, confidentiality and

Table 2. Applicable safety measures for wiki

Feature	Functions
Security	Authentication to avoid malicious user, authorization, message integrity, confidentiality, encryption, and other operational defense facilities and mechanisms.
Privacy	Authorization & verification to collect and store and display personal data. Anonymity, unobservability, pseudonyms, identity management, likability and reputation. Anonymity via implicit addressing on broadcast ad hoc networks. Use of Privacy Enhancing Technologies (PETs) to defend privacy rights.
Trust	Certification authority, authentication, audit. Trusted computing base and support for collaborative environment.
Auditing	Complete auditing system for users. Non-repudiation to avoid denial of documents sent for accounting, legal and forensic reasons. Alert law enforcement agents to investigate further.
Digital forensics	Traceability, accountability, pre-active, re-active and post-active investigation system. Journalizing of events in mobile and non-mobile agent system environment in background real-time mode. Enticement systems to attract fraudulent and illegitimate agents into a honey pot in order to immobilize and prosecute them. Also include tracing and forensics analysis of identity management.
General System Safety	Roll back transaction in case of failure, or playback as defined by law enforcement. Non-mutilation or copying of software agents. System safety, fault tolerance (backup system) and payment safety limits of transactions to ensure availability and reliability of wiki.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 5. Server access control on job title



operational defence (Kannammal & Iyengar, 2007). Meanwhile, there are many security threats potentially threatening wiki such as eavesdropping, spoofing, malicious interception, double spending, uncontrolled cloning, fraud, and audit trail. Thus, security mechanisms have to be embedded to ensure that wiki will not sacrifice security requirements (Furnell et al., 2008).

The basic philosophy behind a wiki is that everyone is permitted to edit everything, but it should be easy to restore the document to its prior state in the case that the modifications are not desirable. The traditional security process is based on detection, prevention and response, where security mechanisms are introduced to prevent unauthorised access to auditing procedures, protected resources and intrusion detection systems are introduced to detect unauthorised use of the system. Finally, a combination of automatic and manual procedures are used to stop unauthorised access and return the system to a consistent state (Jensen, 2009).

Regarding security services our goal is to support them on demand. Therefore, our model can support the following three states according to users' or organizations' specific needs: (a) classic wiki transactions, where anyone can read and write a page, (b) traditional web transactions where everybody can read a page, but only a group of them can edit it and (c) closed project transactions, where only project contributors can read or write pages as illustrated in Figure 5 and explained in Table 3. The information security in wiki has three levels as shown in Table 3.

The system provides the security model to ensure a secure environment for participants to work in an open collaborative authoring system based on wikis. It has been observed that *integrity* and *protection* of information is the most important security property in open collaborative authoring systems (Jensen, 2009).

The system provides the secure migration mechanism base on the username and password which insure if the user is staff, teacher or student. For ensuring the identification of specific user information and data, the system supports the trusted third party authorization mechanisms and permission and role concepts for different actors. Security protection handles the following aspects:

- Availability - services are available to authorized users.
- Integrity - free from unauthorized manipulation.
- Confidentiality- only specific user receives the information.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Table 3. Levels of security

Levels	Phases
Level 0	Anyone can read and write a page without using a password and user name.
Level 1	Everybody can read a page, but only a group of them can edit it who contributed to the project by having a password and user name.
Level 2	Only project contributors can read or write pages by having a password and user name.

- Accountability - the entities must be traced uniquely.
- Assurance - assure that the security measures have been implemented properly.

In addition, the system provides a secure migration mechanism base on the username and password to ensure if the user is operating as staff, teacher or student as intended. For ensuring the identification of specific user information and data, the system supports a trusted third party authorization mechanism to give permission according to role concepts for different actors within the open collaborative environment.

Privacy

Privacy is an expression of self-determination and dignity perceived as a fundamental human right by most constitutions of democratic societies. Personal privacy is largely based on data protection legislations and directives to protect, collect, store and process personal data in order to guarantee privacy. Both legal and technical means have come together to protect privacy and ensure that the individual or the wiki performing on behalf of the individual has explicit control to ensure that right to protect privacy (Patel, 2010).

Nowadays, traditional approaches are not enough anymore to protect the privacy rights of users and address these threats in social computing. The following story is a real example of a privacy invasion which shows the importance and necessity of having a more holistic view. The event occurred while a student felt safe in wiki due to provided option of stay anonymous by withholding his name, but his location information revealed his identity. Wiki allows students to create and edit location linked content; however, pages editors can stay hidden or reveal their identification, the same goes for their location. The student put unpleasant comments about a course professor and revealed his location, but not his identity. Hence, the professor looked into his wiki profile to find the history of page edits; he realized that the comments were added when he was teaching in his classroom. Thus, only two students who were using a laptop during the class were accused and he correctly figured the student's identity out. Consequently, the result was a confrontation which caused the dropping of the course by the student. This example demonstrates how privacy can be preserved by considering social inference/interference risks through this context. It typically includes seven categories of user privacy threats in social computing system (Antoniou et al., 2008; Motahari et al., 2007):

- Inappropriate use by administrators.
- Legal obligations.
- Inadequate security.
- Designed invasion (poor features).
- Social inference with lack of entropy.
- Social inference, interference, implication through persistent user observation.
- Social leveraging of privileged data.

These seven categories give the ability to control what information one indicates about oneself over the wiki environment in education specifically. Therefore, they are essential to be considered in the design of wiki.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Trust

Social computing is about the study of social behavior and context based on computational systems. While numerous online social computing systems/applications are being developed in an unprecedented pace, many issues related to trust management, social computing, and their relationships remain unexplored and unanswered, though they represent major concerns in the cyber community. On the other hand, if information involved in social computing is used properly, it can significantly enhance the trustworthiness of most, if not all, of our social computing applications, and greatly promote social computing in a wide range of contexts.

On the one hand, users may trust some people more than others, therefore will be more influenced by them (Forman et al., 2008). On the other hand, a user will neither trust, nor be influenced by unknown users making recommendations because of the lack of trust and confidence (Leskovec et al., 2006). Golbeck et al. described that the similarity of profile attributes (such as ratings of articles) induces trust among people (Golbeck, 2009). They analyzed data from Article Trust, finding that several profile features beyond overall similarity affect the degree to which subjects trust other users. Based on those studies of the degree to which trust is formed, bidirectional effects on ratings and users trust is readily apparent.

More concretely, Denning et al. enumerates a number of risks associated with the usage of Wikipedia, which are applicable to many other collaborative systems with user-generated content (Denning et al., 2005). These include:

- Accuracy: not knowing which content is accurate; often exacerbated by lack of references.
- Motives: not knowing the motives of editors, who may be biased for various reasons?
- Expertise: not knowing the expertise of editors.
- Stability: not knowing how much it has changed since the last viewing.
- Coverage: spotty coverage of topics.
- Sources: cited information may come from hidden or non-independent source.

In the wiki reference model, all data or information added in the articles or assignments are required to give a reference in order to prove its authenticity. Moreover, each user in the wiki has a metric number which indicates who changes anything in a wiki page. The changes are saved automatically in wiki history. Therefore, all of these are important elements raise the trust in using wiki in education environment.

Audit and Digital Forensics

Auditing, accounting and overall management are important safety components in wiki for e-learning purposes. Even more important is digital forensics as an activity of investigation to trace and analyze illegal and fraudulent events to produce evidence for the purpose of law enforcement. Digital forensics has four modes of operation:

- Post-active: to catch and prosecute the culprit;
- Pre-active: to provide defense mechanisms to prevent illegal events taking place;
- Re-active: to take appropriate course of actions to prevent illegal or unauthorized events from taking place during real-time live operations; and
- Trap-active: to actively entice/attract illegal or fraudulent culprits to fall into a trap like a honey pot so as to immobilize, prevent, penalize and prosecute them (Patel, 2010).

Auditing can be a part of digital forensics or vice versa in wiki management framework. More precisely, in wiki, digital forensics includes event data collection, event data analyzing, employ various protocols to trace and block illegal events or allow controlled actions to take place to follow the illegal pattern without the culprit making any damage and formulate reports to prosecute or defend under law enforcement legislations. The agents

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

carry out the component functions to add a sense of improved intelligence gathering and analysis, confidence and trust, reliability and fault-tolerance not only in wiki collaborative environment but also in all aspects of the digital forensics activities themselves. However, using wiki in digital forensics can cause a few problems. For example, the legitimate right of wiki user acting anonymously conflicts with the rights of a server victim identifying the malicious user (Antoniou et al., 2008). The goal of digital forensic is to collect evidence and reveal the identity of the attacker to the server, as either normal user or real attacker.

DISCUSSION

Wikis underlying platforms, host computers and infrastructures should be trusted, need to be protected from abuse, secured from threats, safe to use, protect the user and provide privacy if necessary, and above all, be identifiable and auditable. The usual approach to simply restricting access to personal data is counter-productive and not suitable for collaborative environments. The primary function of collaborations is to share information not restrict it. Therefore, privacy protection in collaborative environments is more concerned with how data is used and ensuring an entity retains significant or complete control over its personal data. Therefore, assistance as tools, notifications, and accessible information is provided to the members of the collaboration to enable better management of their privacy. Privacy functions are tied to digital forensics and audit on the one side for law enforcement and infringement prevention purposes, and on the other side if it is to achieve better levels of privacy for its end-users. A further risk is that some wiki sites privacy policies effectively require users to give up their rights to privacy. The sites may claim ownership of all content posted on the site in perpetuity, including the right to share the information with third parties. Value of social computing enables him to find information faster on wikis; reduce redundancy and connect to others in intention of finding expertise using professional networking tool. A set of qualitative metrics has to be defined in order to evaluate the encountered threats or violations during the participation in the wiki. This provides confidence in the users to feel comfortable with the learning experience in a satisfactory and beneficial manner.

CONCLUSION

The conceptual key issues and core principles of secure wiki, privacy, trust, implicit addressing, digital forensics and audit grouped together and encapsulated as safety measures were presented. The integrated environment of social computing provided the opportunities to further increase multi-faceted wiki learning collaboration between the members. This required enterprise collaboration with the right organizational structure to ensure that those responsible for learning approaches and social computing are themselves collaborating jointly to manage the wiki learning environment. Wiki has become one of the popular social computing Web-based applications, which is most suitable for collaborative learning compared with forum and blogs.

In summary, to make the audit and forensic services secure and significant to trace normal (non-audit/forensic) wiki, authenticated certificate authority, cryptography techniques and secure protocols have to be implemented. Thus, the authenticity of the audited evidence for the e-learning activities depends on the security, reliability and accuracy of the entire system. Our further work is currently defining the quantitative and qualitative analysis and their metric of the proposed safety measures framework for safe collaborative learning and teaching in the context of social computing.

ACKNOWLEDGMENT

The authors wish to acknowledge and thank Ministry of Higher Education, Malaysia for providing fund to support this research through the Exploratory Research Grant Scheme (ERGS)

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

number ERGS/1/2011/STG/UKM/01/16 and the Long Term Fundamental Research Grant Scheme (LRGS) number LRGS/TD/2011/UKM/ICT/02/01.

REFERENCES

Antoniou, G., Leon, S., Stefanos, C., & Paramalli, U. (2008). Privacy and forensics investigation process: The ERPINA protocol. *Journal of Computer Science & Interface*, *30*(4), 229–236. doi:10.1016/j.csi.2007.10.008

Aronsson, L. (2002). Operation of a large scale, general purpose wiki website. In *Proceedings of the 6th International ICCC/IFIP Conference on Electronic Publishing*, Karlovy Vary, Czech Republic.

Borselius, N. (2002). Mobile agent security. *IEEE Intelligent Systems*, *14*(5), 211–218.

Charron, C., Favier, J., & Li, C. (2006). *Social computing: How networks erode institutional power, and what to do about it*. Cambridge, MA: Forrester.

Clarke, R. (2001). *Privacy as a means of engendering trust in cyberspace*. Retrieved May 2, 2012, from http://www.anu.edu.au/people/Roger.Clarke/DV/eTrust.html

Denning, P., Horning, J., Parnas, D., & Weinstein, L. (2005). Wikipedia risks. *Communications of the ACM*, *48*(12), 152–152. doi:10.1145/1101779.1101804

Forman, C., Ghose, A., & Wiesenfeld, B. (2008). Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets. *Information Systems Research*, *19*(3), 291–313. doi:10.1287/isre.1080.0193

Furnell, S., Katsikas, S., Lopez, J., & Patel, A. (2008). On mobile wiki systems security. In Furnell, S., Katsikas, S., & Lopez, J. (Eds.), *Securing information and communication systems: principles, technologies and applications*. London, UK: Artech House.

Golbeck, J. (2009). Trust and nuanced profile similarity in online social networks. *ACM Transactions on the Web*, *3*(4), 12. doi:10.1145/1594173.1594174

Jensen, C. D. (2009). Security in wiki-style authoring systems. In *Proceedings of the Third IFIP WG 11.11 International Conference on Trust Management III* (Vol. 300, pp. 81-98).

Kannammal, A., & Iyengar, N. C. S. N. (2007). A model for mobile agent security in e-business applications. *International Journal of Business and Information*, *3*, 129–134.

Lazar, I. (2010). *Merging the worlds of social computing and unified communications*. Retrieved May 5, 2012, from http://www.networkworld.com/community/blog/merging-worlds-social-computing-and-unified-c

Leskovec, J., Adamic, L., & Huberman, B. (2006). The dynamics of viral marketing. In *Proceedings of the 7th ACM Conference on Electronic Commerce*, Ann Arbor, MI.

Li, X., Mao, W., Zeng, D., & Wang, F. Y. (2008). Agent-based social simulation and modeling in social computing. In C. C. Yang, H. Chen, M. Chau, K. Chang, S.-D. Lang, P. S. Chen, et al. (Eds.), *Proceedings of the International Workshop on Intelligence and Security Informatics* (LNCS 5075, pp. 401-412).

Motahari, S., Manikopoulos, C., Hiltz, R., & Jones, Q. (2007). Seven privacy worries in ubiquitous social computing. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, Pittsburgh, PA.

Musser, D., Wedman, J., & Laffey, J. (2003). Social computing and collaborative learning environments. In *Proceedings of the 3rd IEEE International Conference on Advanced Learning Technologies*, Athens, Greece

Newsgator. (2009). *Delivering ROI with enterprise social computing*. Retrieved May 5, 2012, from http://www.newsgator.com/LinkClick.aspx?fileticket=mIFywjDmIEA%3D&tabid=98

Patel, A. (2010). Concept of mobile agent-based electronic marketplace – safety measures. In Lee, I. (Ed.), *Encyclopedia of e-business development and management in the digital economy* (Vol. 1, pp. 252–264). Hershey, PA: Business Science Reference.

Schuler, D. (1994). Social computing. *Communications of the ACM*, *37*, 28–29. doi:10.1145/175222.175223

Thite, M. (1999). Leadership: A critical success factor in IT project management. In *Proceedings of the International Conference on Management of Engineering and Technology* (Vol. 2, pp. 298-303).

Wang, F. (2005). Social computing: A digital and dynamical integration of science, technology, and human and social studies. *China Basic Science*, *7*, 5–12.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Ahmed Patel received his MSc and PhD degrees in Computer Science from Trinity College Dublin (TCD), specializing in the design, implementation and performance analysis of packet switched networks. He is a Lecturer and Consultant in ICT and Computer Science. He is a Visiting Professor at Kingston University in the UK and currently lecturing at Universiti Kebangsaan Malaysia. His research interests span topics concerning high-speed computer networking and application standards, network security, forensic computing, autonomic computing, heterogeneous distributed computer systems and distributed search engines and systems for the Web. He has published well over two hundred technical and scientific papers and co-authored two books on computer network security and one book on group communications, co-edited a book distributed search systems for the Internet.

Mona Taghavi received her BSc degree in Information Technology from Parand Islamic Azad University of Iran in 2007. Besides her involvement in several Iranian national ICT research projects, she had worked for an IT consulting and project managing company which was responsible for overseeing the Supreme Council of Information and Communication Technology (SCICT) of Iran programme. She was responsible for preparing some of the technical reports for this programme. Currently, she is pursuing her MSc in Management Information Systems and Network Security at University Kebangsaan Malaysia and undertaking research in cooperation with Prof. Dr. Ahmed Patel in advanced secure Web-based information systems. She has published 10 papers and she is a reviewer for the Computer Standards and Interfaces Journal.

Joaquim Celestino Júnior received his MSc degree from Federal University of Campina Grande, Brazil, in 1989, and his PhD degree from University of Paris VI, France in 1994 in computer networks. He was postdoctoral researcher at Columbia University in 2009-2010. He is a Professor in the Department of Computer Science at State University of Ceará in Brazil and Head of the Computer Network and Security Laboratory (LARCES). He has published more than one hundred technical and scientific papers and co-authored several books. He is currently involved in the R&D of VANETS & MANETS, Sensor Networks, Cloud Computing and Network Management and Security. He is involved in many TPCs of conferences and reviewer of many scientific journals and conferences.

Rodziah Latih received her BSc degree in Computer Science from Universiti Kebangsaan Malaysia in 1993 and MSc in Software System Technology from Sheffield University, United Kingdom in 1996. She had led several projects funded by Universiti Kebangsaan Malaysia and Malaysia Ministry of Science Technology and Innovation. Currently, she is pursuing her PhD in Advance Software Methodology at University Kebangsaan Malaysia and undertaking research in Web Mashup Development Approach and Computer Programming Pedagogy.

Abdullah Mohd Zin received his BSc Hons from University of Southampton, MSc from University of Wales and PhD degrees in Computer Science from University of Nottingham, United Kingdom. His main area of specialization is in specializing in formal approach in software engineering. Apart from that he is also interested in the area of platform technology and teaching of programing. Currently he is the dean and Professor of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. He has published over one hundred technical and scientific papers.

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.