Social Networking: Cyber Communities and Security Issues

Shaftab Ahmed
Software Engineering Department
Bahria University, Islamabad, Pakistan
email Shaftab_2010@yahoo.com,

Abstract -- **The world is experiencing a smart change of life style as a result of a wide range of developments in the information and communication technology (ICT) sector. The computation and storage centers are vanishing in the cloud domain leaving human communication interface as the only requirement for using these resources. Evolving cyber communities (CC) are groups of users having common interest areas. Information sharing across such communities is easily possible which, leads to more complexity and vulnerabilities. The platform independent applications in service oriented architectures (SOA) over the web offer a variety of opportunities for users of all walks of life. They are able to create mashups integrating different applications and services to suit their requirements. Cloud service providers (CSP) extend the social network applications for information collection and conducting surveys for business and marketing strategies. Internet of things (IOT) is a concept to converge data, process and people to extend business applications in virtual domain. ICT applications over cloud architecture are ubiquitous and pervasive; developers are extending the concept to develop smart city and smart home architectures for the future. In this paper, we address the challenges offered by growing interest in social networking and ease of information availability for applications in virtual domain. Various new issues have to be carefully studied as the component of human interaction has to be controlled besides the information security to avoid miss use of information.**

Keywords—Service Oriented Architecture (SOA); Information and Communications Technology (ICT); Internet of Things (IOT); Cloud Service Provider (CSP); Cyber Communities (CC)

I. INTRODUCTION

Mobile communications, networking and Internet based solutions for virtualization and resource sharing have given birth to a new life style through social networking. The participation of humans of all ages, professions and interests has given rise to formation of cyber communities. Community is a group of users sharing common interest for example content creators, users, developers and service providers, etc. form communities spanning social networks [1]. Hence, a community in the ICT domain may be seen as interlinked web pages in the Internet cloud. Social networks like LinkedIn, Facebook, Tweeter, WhatsApp, etc. have assumed importance for sharing information in professional and social groups or communities. These communities are usually able to interact with each other hence, making bigger picture of social networking. Whereas it is an interesting phenomenon, it is often complicated and dangerous [2].

The cyber communities (CC) usually have no restriction on membership and cross community information sharing. Hence, explicit and implicit communities may be formed. The implicit communities are difficult to control and monitor for content distribution, etc. Some methods are available to ensure privacy of information between participants of the groups but it is not effective when a group member may provide information knowingly or unknowingly to others which, may eventually be compromised. The social network users need to be educated on the weaknesses of global phenomena of social networking. The user must understand that all information placed in a social network is vulnerable so it should be carefully selected before sharing [3]. As the members present them in virtual domain it is often difficult to differentiate genuine or fake information. Hence, making judgment for selecting a member in a community is usually difficult.

Cloud services virtualize the platform and infrastructure to be used by clients through software. It offers infrastructure as a service (Iaas), platform as a service (Paas) and software as a service (Saas). Lately a new term IT as a service (ITaas) has also been introduced. Cyber communities enlarge their scope through a marriage of cloud computing and social networking [4]. Social network users may access information available in the cloud through service oriented architecture [5]. ICT tools are often used to extract information from social networks and cyber communities related to market trends, evaluation of strategies to forecast and setting targets for future.

Human reliance on the information systems hosted on the web has led to development of community based computing infrastructure or Community Cyber Infrastructure (CCI) in which, the information discovery and extraction is performed through various ICT technologies. National Science Foundation (NSF) defines Cyber Infrastructure (CI) as integration of computing, data networks, digitally enabled sensors, observatories, experimental facilities and interoperable suit of software and middleware services [1][6]. Cyber enabled Discovery and Innovation (CDI) is an initiative of NSF to develop a new generation of computationally based discovery concepts and tools to deal with complex data rich interacting systems. The discovery of information may be from structured (conforming to a schema) or unstructured (not conforming to a schema) data sets.

In Section II, we review related work. In Section III, social networking, cyber community and supporting technologies are discussed. In Section IV, the security issues in cyber communities are highlighted. In Section V, research work

 ISBN: 978-1-61208-521-0

initiated is presented. Finally, in Section VI, the paper is concluded with discussion on challenges and future trends.

II. RELATED WORK

Social networks are attacked in mainly of two ways. First, manipulating executable code to gain access or be able to install malicious software. Secondly, the human hackers exploit personal information gathered by peeking and poking the social network. Sometimes, a passive listener is installed to gather information useful to attack a social network [7].

The data posted on the social media is not limited to malicious software attacks; the cyber criminals may mine networks to obtain persisting useful information, and use it to steal intellectual property, highjack a website or compromise company profile. Often data remains available in various cache buffers even after a user has logged out; malicious users may get access of this data intelligently [8]. Most enterprises have adopted security and firewalling schemes to control and filter malicious activities. Social networks open a new window where employees of a company may un-intentionally expose useful information in public domain leading to exploitation or financial losses to the enterprise.

Social network users must bear in mind that information posted on a social network is no longer private. However secure the site may be yet the information can be easily leaked either by a member or through a loop hole in the security mechanism [9]. Some of the tactics used are as under:

Click-jacking:	Concealing hyperlinks beneath a visible link
Cross –Site Scripting:	Injecting client side script into web page
Doxing:	Publically releasing identity information and pictures, etc.
Pharming:	Redirecting to fraudulent sites to extract personal data
Phishing:	An email or other content often sent on behalf a known user containing a malicious link
Phreaking	Gaining unauthorized access to telecommunication device also call physical theft.
Spoofing:	A passive listener to gather information to be used for exploitation

Business communities are using social media to extract useful information for marketing strategies and human resource management. For example [10] Linked in is being used for hiring skilled manpower. Business to business communications has strengthened collaboration for increase in productivity of a company due to broader area of exposure. The developers and service providers offer large storage spaces over the cloud e.g., S3 of Amazon. According to a recent survey [11] the commercial enterprises are not comfortable with the virtualization of storage for confidential information; they would prefer to explicitly know the location / custody of confidential data. To build their confidence it is important to implement proactive security strategies, effective user policies and reinforcing methods to monitor and protect enterprise resources [10]. The employees often use social networks while at home or work place; it is recommended that regular training on security issues and company policies should form a part of the policy. The network at home is usually not adequately protected hence, important information may be compromised.

The social networks have a niche market in e-Healthcare, and education sectors because of direct human involvement. Developers are providing all time guidance and help to patients through social media; often warning messages and other useful information is provided to the community.

III. SOCIAL NETWORKING AND CYBER COMMUNITY AND SUPPORTING TECHNOLOGIES

Social networks virtualize the usage of resources through applications used to interact with them. A typical social network is based on layers of abstraction, shown in Figure 1 where the human interface for user registration is the highest layer; followed by service registration and discovery mechanisms setup by service provider. The services are virtualized through tools for query, access control, data management and visualization. Resource virtualization presents the physical hardware and networks in a cloud hiding all the complexities and offering a service oriented architecture. The social networks allow users to form communities which, may be overlapping in terms of interests and users. Various controls over such groups are also provided to share or present only the authorized information. Some of the enabling technologies have been shown in Figure 2.

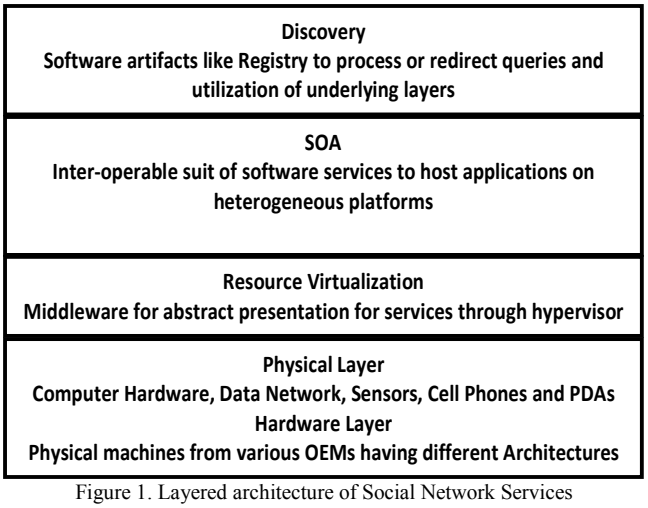

Figure 1. Layered architecture of Social Network Services

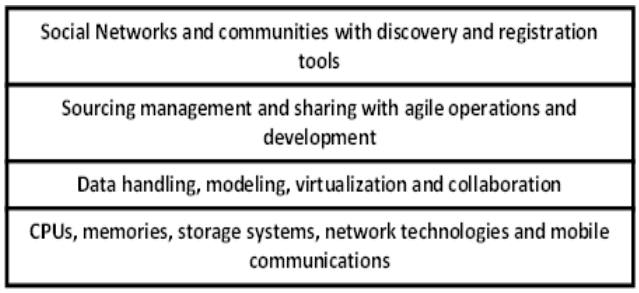

Figure 2. Enabling technologies for social networking

A. *Social networks implementation*

The growth of communities in social, healthacre, medicine and hundreds of others, has been possible as a result of developments of service oriented architecture (SOA) offered through web engineering and data communication networks. Service oriented architecture is used for abstration, low cohesive concepts for data mangement and presentation [5]. The services offered are recorded in a registry which, is looked up for selection. The discovery tools hosted by social networks facilitate selection of desred services. Web engineering is vital in abstracting the underlying network and communication systems. Hence, social network users may interact with virtual environments without being a computer literate. Lately cloud storage and archiving services are being offered by all the mobile commmuications companies used for availability on anywhere anytine basis through smart phones or PDAs.

B. *Cloud computing offered to social networks*

An emerging field in ICT domain is social networking conceived to exploit the ubiquitous nature of social networks and cloud services offered through various web sites. The users are able to share resources and use cloud services for creating mashups. A mashup application blends services for data, presentation and functionality. It also allows integration of different APIs in a single application. For example Facebook users can make applications hosted by a CSP like Amazon [12][13].

Volunteer computing is a distributed computing resource like SETI@Home, Storage@Home and Folding@Home. The experience of such sites can be used in social networks to provide enormous computing power and storage space through collaboration of IT communities [14]. Some examples of potential applications are:

- Document sharing by Google Docs and Zoho
- Pictures and video sharing by Piccasa and Flicker
- Location based services like Google Maps and Bingo Maps
- Context aware applications using mobile mashup services using memory enabled sensors, touch screen, cameras, GPS and accelerometer, etc.

C. *Social Networks and technology developments towards smart homes and smart cities*

The world is experiencing a fundamental change in social setup and lifestyles. The popularity of smart phones and all time Internet connectivity through wireless, Wi-Fi and WiMAX technologies has motivated technology developers to introduce a new concept of smart homes and smart cities. Some examples are smartcities of IBM [15], sustainable-cities of Siemens [16], citynext of Microsoft [17] and mycity of atos [18].

Smart cities require development of tools to address cross domain communication for information sharing and distributed computing. Such solutions have to cater for a variety of features and perspectives in modern society. The developers are in pursuit of tangible services and solutions for the social networks mostly ubiquitous and pervasive. Innovative solutions and new ideas are being matured to meet the requirements of smart homes especially for aging population [20].

Internet of Things (IOT) is a concept to converge data, processes, people, and business system providing an opportunity to extend business scenarios [21][22]. Cloud Service Providers are offering services to build and deploy smart city projects in real world to evaluate the potentials / weaknesses and devise methods to meet new challenges. For example Microsoft Azure services may be used to monitor assets for operational performance improvement and provision of innovative solutions through data analysis and business models [23]. Home care and e-Healthcare models are being rapidly developed to provide better quality of life, protection and health monitoring. The elder populations, patients getting prolonged medical treatment or requiring post-surgical monitoring are clients for smart homes and smart cities [24] [25]. A cyber-home connected to a service provider over the Cloud architecture is shown in Figure 3.

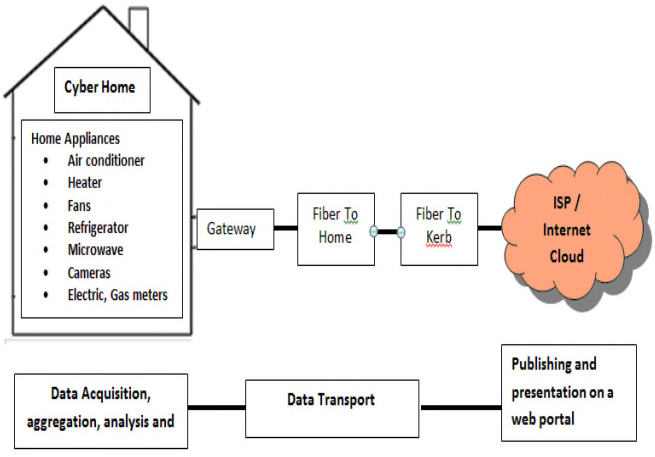

Figure 3. Smart applications in a cyber-home

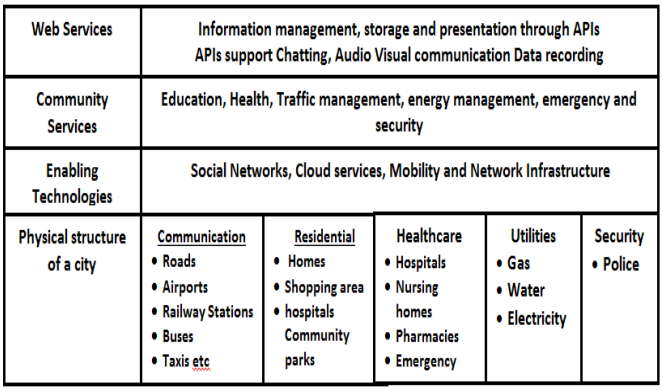

Figure 4. IOT Smart city architecture

D. *Web and open access to learning and role of social networks*

Web 2.0 technologies promote effective use of collaborative network operation for information sharing and interactive learning [26]. The open access learning oportunities are available for integrated professional education. Open access helps break the barrier between instructor and student to promote academic learning. Shulman [27] states, "learning is useful when it is private and hidden; it is most powerful when it becomes public and commercial". Other scholars have emphacized the benifits of public learning and are of the view that, "open source" and "open access" software resources have been instrumental in generating useful academic activities and promoting innovative ideas [28].

ICT has experienced rapid development of open source tools including bulletin boards, courseware, portals and content mangement software for open access learning environments [29]. A number of institutions and research groups have used open sharing, mutual aid and knowledge disseminstion concepts to promote establishment of free e-learning resourses [30].

IV. SECURITY ISSUES

A. *Cyber Domain of Social Networks*

The social networks are ubiquitous and pervasive; they have wide acceptability in communities shaped by human interest and social information interchange extending homes and offices into virtual domains. It has been observed that developers often use these networks for information gathering for their business and marketing applications. The information is live instead of old documented surveys so it is good for dynamic market engagement.

Hence, social networks strengthen connectivity, attract and engage customers to get inputs for devising strategies for the company. However social networks are easy targets for malicious activities. Often users expose themselves unnecessarily in social communities without releasing that their data or communication may be misused. Hence, it is extremely important to educate social network users about the risks and pitfalls that they have to watch out for fruitful experience and avoid embarrassment [31].

B. *School communitity concerns regarding networking*

Besides private, business and commercial organizations a large community affected by social networking is the students. Schools are integral part of society today; where besides academic activities, meetings and counseling sessions of teachers, parents and students are conducted to enhance academic performance and reduce discipline problems. The online environments are easily accessible to students of all levels; hence they are causing new problems in society and learning environments. While controlled online activities within a school may ensure safe usage to some extent; the students may use the networks from home or other places leading to serious problems.

It is necessary that school and community policy makers should realize the severity of problems associated with learning communities; where the students need parenting and guided use of information. It is necessary that comprehensive school wide and community wide policies should be made for collaborative management through training, sharing of information and introducing guidelines for safe schools and neighborhoods

C. *Limitations and vulnerabilities*

Social network users are inclined to have trust relationships and informal communications instead of well thought of and well-grounded business communication The sites encourage users to share personal information, photos and videos, opinions and comments or tagging which, is source of enjoyment. They are usually unaware that in spite of careful information sharing in restricted groups; the vulnerability of host site may compromise their information leading to misuse by cyber-criminal. Some of the scenarios are as under [32]:

i. A friendly looking website may incite a user to divulge his profile information and personal detail which, can be used by malware [7].
ii. The user may be fooled by a masquerading attack where he might engage with a cyber-criminal
iii. A community member may turn to be not trustworthy; he may expose the information unsafely
iv. The nonprofessional employees of a company are often unaware of the importance of exercising privacy in company details and secrets. If not properly trained they may help malware to break in the security barriers of the company. Some experts emphasize that periodic training and briefing is necessary for both professional and nonprofessional users. A professional user may forget that he is using the laptop of the company while at home; or visit a social network through his official mobile, etc.

 ISBN: 978-1-61208-521-0

v. Email spams are used for marketing of products and utilities; a user may be tempted to click a link, leading to malicious activity besides going to the website.
vi. Human resource managers are often using social networks to acquire profiles and professional detail of applicants. The negligence in maintaining this information may compromise the detail; for misuse by cyber-criminal.
vii. The website pages may have some security flaws which, may be identified by a hacker for misuse. Such incidents have been reported for Facebook and Tweeter where suitable measures were taken by them

D. Some of the concerns of using social networks:

The user experience with social networks has revealed many weak areas which, need to be addressed by the developers and managers of social networks. This is especially important in the evolving scenario of social network hosting in cloud domains. The iCloud, Google docs, etc. are a few of the important ones. They may have an overlap with social network activities.

A few weak areas to watch out are as under:

- No restriction on membership of social network
- No check on creating an official site hence, can be misused to create fake institutions
- Judgment of friend or foe in cyber network is difficult; users have to be educated on how to ascertain that he is communicating with a genuine member
- Cross community information sharing; either it should be restricted or sufficient controls and forensic data management should be enforced so that information may not land into irresponsible hands after legitimate usage
- Loss of control over information shared may lead to wrong reporting or making it controversial; hence, users in a community or an enterprise should be educated to avoid putting all information on the social site. An option to leave or migrate from the host site gracefully should be kept in mind
- Information sources like email, blogs, Twitter, Facebook and Myspace increase visibility in communities and widens the scope but overloads the educators and may be annoying in some cases.

E. Attack on host or computer network

Social networks weakness is not the only source of cyber attack [33]. The host network or service provider in virtual domain may also be hit by cyber-criminal compromising all the information of the clients maintaind on it. In such cases, the social services may suffer severely hence, the enterprises using social networks should have proactive strategies in place to handle such situations.

F. Recommendations and guidelines for secure use of social networks

Detailed study of social networking sites, discussion with user communities, entrepreneurs, students, scientists, researchers, medical professionals, etc. has revealed that the awareness of security threats is not adequate. We recommend that suitable measures should be adopted for their education as under:

- Self awareness of suitability of sharing information
- Avoid third party usage of account
- Treat everything is public; the world not only your closed community may be seeing the information shared
- Protect yourself protect others or the community by not allowing information to across to other communities without suitable authorization
- Campagn to educate social network users and administartors for rational usage and abiging by security policies.
- A regulatory framawork maintaining forensic data for social network is becoming important so that suitable measures can be taken to fix responsibility for unauthorized usage or informatin leak
- Stronger authentication and access control methods have to adopted to discourage BOTs by using captchas or other methods
- Provision of suitable tools to revoke user accounts as well as edit or remove profiles from the posts should be available
- The social networks should use filtering tools to establish legitimacy of information and forbidden content distribition

V. RESEARCH WORK

We have chosen e-healthcare, e-learning and business communities as domains of interest for research work. It is understandable that collection of useful social interaction data is instrumental for assessment and analysis. However, while using popular social networking sites, there are two issues i.e.

i) Non availability of data from popular sites
ii) Non serious activities are more common

Since we intend to focus on three domains (e-healthcare, e-learning and business), which require useful and extensive data, we will develop social networking facilities of our own. These sites will be available to the closed communities in the above said domains

The first two domains are human centric where sharing personal data and experiences securely is of prime importance. The third has a wide perspective where the market trends, user experiences etc., are used for making strategies to market products and human resource management etc.

 ISBN: 978-1-61208-521-0

In healthcare and patient handling / rehabilitation, the data collected from the patient history and interactive sessions will be used for treatment, rehabilitation, nutrition plans, etc. Learning communities have a wide perspective; however, we will focus on schools first. We aim to bring parents, teachers, students and policy makers together, through social network for learning, parenting, teaching and socialization. They may evolve strategies to be adopted for upbringing of children in highly volatile ICT induced information overload. Our forum will promote shared vision, communication without barriers and collaboration towards achieving common goals of education and integrated society.

For business community product marketing and human resource management have been identified. We intend to perform behavior analysis of social network users with respect to thoughts, daily routine, likes, dislikes etc. The data collected about market requirements, human consumption alongwith end user comments on social sites will be used to predict future trends and plan product marketing. Intelligent use of data available on other competitors / manufactures sites regarding their products and end user feedbacks will be used to derive competitive advantage.

For human resource management, the data will be collected through social networks and processed to help entrepreneurs in making strategies for carrier planning, hiring and granting relief or bonus for employees / shareholders. Managers may use the new applicant's data to prepare suitable probing questions before formally interviewing individuals.

While developing the above said model applications we will focus on vulnerabilities of the data collected and shared between communities. Suitable measures will be adopted, alongwith educating the users for safe usage of social networks through recommended policies, guidelines and safe practices for safe use of social networks.

VI. CONCLUSION AND DISCUSSION

Social networks are being used for business purposes for human resource management, marketing, forecasting etc. Trends indicate that the phenomena of increasing interest and usage of social networks in all walks of life will rapidly increase in future. It is important to avoid pitfalls and threats while reaping the benefits of social media. The business models need to be carefully developed through clearly articulated procedures, policies and role of users in various departments, guests and members from outside. It implies that clarity on what information can be posted on which, site and by who should be ensured. It is equally important to devise remedial strategies, in failures before engagement in social network.

The employees of a business enterprise are the weakest link which, is usually exploited by the cyber criminals. For example a careless download by an individual on his personal computer or mobile may be used to compromise important resources of an enterprise. Similarly an employee may innocently post information following a link helping malware to break the cyber defense of a company. It is recommended that companies using social networks should evolve a continuous training program for employees demonstrating threats and their impact. Furthermore, these sessions should include all the IT employees not just those who matter.

Social networking has significantly changed human life cycle, business models and the level of awareness / dependency in digital world today. It must be realized that opportunities offered by social networks should be tapped cautiously realizing risks and devising suitable strategies / counter measures for smooth running of an enterprise.

VII. REFERENCES

[1] A. Elmagarmid, A. Samuel and M. Ouzzani," Community Cyber Infrastructure Enabled Discovery in Science and Engineering", RPI, Troy, NY, September 2007

[2] R. Kumar, P. Raghavan, S. Rajagopalan and A. Tomkins "Trawling the Web for emerging cyber-communities" 1999, pp 402-415, Published by Elsevier Science B.V. doi=10.1.1.387.3453

[3] S. A. de Chaves, C. B. Westphall, C. M. Westphall, and G. A. Gerônimo, "Customer Security Concerns in Cloud Computing" IARIA, 2001, pp. 7-11 ISBN 978-1-61208-113-7

[4] D. Fu, J. Zhu and G. Dasmalchi," IT as a service Cloud Computing" IBM Alliance at Cisco Systems Cisco Systems, IT Pro March/April 2009 Publ ished by the IEEE C omputer S ociet y, 1520-9202/09, 2009 IEEE, pp. 10-13

[5] L. Ngo, " Service-oriented architecture for home networks" TKK T-110.5190 Seminar on Internetworking 2007-3-4/5

[6] M. McDowell and D. Morda, " Socializing Securely: Using Social Networking Services", Carnegie Mellon University. Produced for US-CERT, a government organization 2007.

[7] S. Abraham and I. Chengalur, "An overview of social engineering malware: Trends, tactics, and implications" Technology in Society 32 2010, pp 183–196 doi:10.1016/j.techsoc.2010.07.001

[8] S. Singh , R. Bagga, D. Singh and T. Jangwal," Architecture of mobile application, security issues and services involved in mobile cloud computing environment", India International Journal of Computers and Electronics research, www.ijcer.org ISSN2278 August 2012, pp 58-67

[9] Mike Gotta, " Risks & Benefits of More Open Social Networking", Burton Group, http:// www.burtongroup.com

[10] F. Lin and C. hung, C. , "Developing and Evaluating the Social Network Analysis System for Virtual Teams in Cyber Communities" Proceedings of the 37th Hawaii International Conference on System Sciences – 2004

[11] A. L. Beberg and V. S. Pande2 ,"Storage@home: Petascale Distributed Storage" 1-4244-0910-1/07 2007 IEEE

[12] A. Mohaisen, H Tran, A. Chandra and Y. Kim, "Social Cloud: Using Social Networks for Building Distributed Computing Services" doi=10.1.1.232.1553

[13] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks", DOI 10.1109/CLOUD.2010.28 IEEE Computer Society, 2010, pp 99-106

[14] S. S. Sivan and S. Durga, " A Survey on Accessing Cloud Services in Social Networks" International Journal of Advanced Research in

Computer Science and Software Engineering, Volume 4, Issue 1, ISSN: 2277 128X , January 2014, pp784-787

[15] http://www.ibm.com/smartercities

[16] www.siemens.com/sustainable-city

[17] http://www.microsoft.com/en-us/citynext

[18] http://www.oracle.com/us/industries/public-sector/national-local-government/city-platform/index.html

[19] http://atos.net/en-us/home/your-business/government-and-cities/mycity.html

[20] H. Chourabi et al," Understanding Smart Cities: An Integrative Framework" 45th Hawaii International Conference on System Sciences, 978-0-7695-4525-7/12 IEEE, 2012, pp 2289-2297, DOI 10.1109/HICSS.2012.615

[21] D. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything" Cisco Internet Business Solutions Group (IBSG) 2011

[22] J. Gubbi, R. Buyya, S. Marusic and M Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions" Future Generation Computer Systems Volume 29, Issue 7, September 2013, pp-1645–1660, http://dx.doi.org/10.1016/j.future.2013.01.010

[23] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stößer "Business models in the service world" IT Pro March/April 2009 Publ ished by the IEEE C omputer Societ y 1520-9202/09, 2009 IEEE, pp-28-33

[24] A. Venkatesh "Smart Home Concepts: Current Trends" CRITO, doi=10.1.1.125.8597

[25] M. Shanmugasundaram, G. Muthuselvi and S. Sundar, " Implementation of PIC16F877A Based Intelligent Smart Home System, ISSN : 0975-4024 Vol 5 No 2 Apr-May 2013, pp 1608-1624

[26] R. Guha and D. Al-Dabass, "Impact of Web 2.0 and Cloud Computing Platform on Software Engineering" International Symposium on Electronic System Design 2010,978-0-7695-4294-2/10 IEEE Computer Society, 2010, pp 213-218, DOI 10.1109/ISED.2010.48

[27] L. Shulman, "Taking learning seriously, Change: The magzine for Higher Learning", 31:4 March 2010, pp 10-17, DOI:10.1080/00091389909602695

[28] N. Jackson. "E-learning material and open access" 18th BILETA Conference: Controlling Information in the Online Environment, April 2003, QMW London, http://www.bileta.ac.uk/03papers/jackson.html

[29] K. Mentor,"Open source and open access: Alternatives to hidden learning environments", 20th annual conference on distance teachning and learning, http://UNWEX.edu/disted/conference, 2006

[30] J. Jiang "Web-Based Open Access for Wide Learning Platforms" 978-1-4244-4507-3/09, 2009 IEEE

[31] http://www.nsa.gov/snac, "Service Oriented Architecture Security Vulnerabilities Web Services" Systems and Network Analysis Center Information Assurance Directorate

[32] "Security: Protect Your Service-Oriented Architecture Network" Cisco Systems 2008, pp1-7.

[33] D. Sancho "Security Guide to social networks" white paper, Trend Micro

 ISBN: 978-1-61208-521-0