IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Use of Social Media in e-Governance: A Study Towards Special Reference to India

M. I. Sandhi[1*], D. Hiran[2], N. I. Modi [3]

[1]Pacific Academy of Higher Education & Research University, Udaipur, INDIA
[2]Faculty of Computer Application, Pacific Academy of Higher Education & Research University,Udaipur, INDIA
3 I/c Head, Post Graduate Diploma in Computer Application, Department of Computer Science, Henchandracharya North Gujarat University, Patan, INDIA

[*]*Corresponding Author: idrish.mca@gmail.com, Tel.: +91-99242-68336*

DOI: https://doi.org/10.26438/ijcse/v7i5.724733 | Available online at: www.ijcseonline.org

Accepted: 20/May/2019, Published: 31/May/2019

***Abstract*—** This paper attempts to analyze the current use of social networks and their promising advantages for electronic governance in governmental organizations. Discuss potential problems, especially issues related to the security and privacy of people, Employees, infrastructure and data that prevent the successful implementation of social networks for electronic governance. Examine India's governance framework project to integrate social media into the organizational structure and examine those issued guidelines for the platform to be used, authorization to participate on behalf of the government organization, scope and extent of said commitment, etc. Compare these guidelines with similar patterns from other nations in terms of access, account management, acceptable use, employee conduct, content, security, legal issues and citizen behavior list its merits, demerits and scope for future improvements.

***Keywords*—**: e-Governance; Social Media; Social Media Policy; Social Media Framework

I. INTRODUCTION

Social media provide users with a rich and deep experience for participation, interaction and collaboration. Several social networking tools allow their users to create and share information on the web and collaborate with others. Interactively making it easier to find information and connect in line with each other. Social media have also been used for online learning, since they have created opportunities for effective learning of teachers, students of learning and Teacher-teacher communication, interaction and collaboration. With the inclusion of mobile technology, there is not only has there been an intense increase in the number and type of social media tools, but its use is also increasing. In developed countries such as the United States, Poland, the United Kingdom and Korea in At least four out of ten adults use social media tools. Social media sites dominate the use of the Internet in Asia and the Pacific [1-2]. Compared to men, women are Participate more actively in social networking sites [1-2]. Even though currently the use of social networks is more popular among young people, but studies are revealing that there are growing trend of participation by the elderly of the past few years. In general, social media can be classified in the following four categories: 1) online networks and ecosystems, for example, Facebook LinkedIn, MySpace and Twitter 2) online publications, for example, YouTube, Flicker, RSS, SlideShare and Twitter, 3) Online collaborative platforms. -e.g. Wikis like MediaWiki, blogs like Wordpress or Blogger, and collaborative office solutions such as Office365, Google Docs, MS Lync, Debategraph, Teamwork or WorkSpot and 4) online comment systems, for example, voting and debate, rating and comments, surveys, surveys, blogs, etc. Online networks and ecosystems build and Reflect networks and relationships between peers. Online publishing tools provide services or platforms for Share and publish content online. The Collaborative platforms facilitate cooperation and work processes among people. Tools for online comments facilitate entry of an audience through one-way or two-way communication. To promote business many organizations have including social networks in its organizational structure. Governments of several nations have also incorporated However; social networks in electronic government make this integration safe and more efficient than they have thought up. Frameworks, policies and guidelines that regulate integration. The IoE has a most important influence on the Big Data background. The key awareness on IoE data science evolution is that every IoE object has an identifier and connects to each other. Now, bearing in mind the circumstances of trillions of such connections that may be producing massive volumes of data (IoE big data), and the competence of current data science and knowledge analytics mechanisms are going to be

challenged [24]. The rest of the article is organized as follows: Section I presents the introduction of the terms. Section II. Briefly presents the current use of social networks in electronic government, followed by discussions about their potential benefits and risks involved in Sections III and IV, respectively. Section V presents the highlights of a recent study that analyzed 26 social media documents. In Section VI, the central elements of a successful social networking policy are listed. In Section VII, the framework of the Government of India and The guidelines for the use of social networks in electronic governance are: examined and its limitations are listed in Section VIII. Finally, Section IX provides guidelines to improve this. Framework followed by conclusion.

II. SOCIAL MEDIA IN E-GOVERNANCE

Commercial organizations, academic institutions and individuals widely use social media for online presence, the promotion of goods and services, the collection of customer comments, the exchange of experiences, interactions with consumers and customers, the collaborative preparation of content, e-learning, communication, social interaction, etc. Recently, politicians, citizens and governments around the world. balloon including those from less developed countries have demonstrated effective use of social media tools to revolutionize government agreements, mobilize movements against and in support of governments, conduct electoral campaigns, maintain communication between the government and citizens in disorder, etc. Barack Obama and Mitt Romney they have actively embraced Twitter and have used social networking sites as campaign tools during the 2012 presidential contest to communicate directly with supporters and, what is more important, to boost the political conversation in a road that goes far beyond the site. Governments under some policy or government officials on their staff. The capacity has been using social networks for foreigners. Matters, administration and information. USA and UK Governments in addition to others such as Australia and Sweden are More active in the use of social networks for digital diplomacy. Currently, 66 percent of all US government agencies. UU They use one or another form of social networking website [1]. According to the UN e-Governance 2012 survey [3], 48 percent, that is, 78 member states provide a us on Facebook "or statement" follow us on Twitter "in your government websites. According to the same survey 7 The percentage of such websites provides chat rooms or instant messaging features to gather public opinion. In India, several ministers and Officials actively use social media to communicate with the citizens.

Recently, Prime Minister has also showed his presence on Twitter while his office launched his Initiative of social networks through Twitter (http: // twitter. com / #! / pmoindia), You Tube (http://www.facebook.com/ Pages / Indian-Prime-Ministers-Office / 107934225905981) and Facebook (http://www.youtube.com/user/zPMOffice India? Ob = 0 & feature = results_main). Similar efforts have been initiated by several other ministries and other government officials throughout the country.

III. ADVANTAGES OF USING SOCIAL MEDIA IN E-GOVERNANCE

Several impediments to the adoption of electronic governance include lack of knowledge of electronic services [4], access to services [5-6], citizens' interest [7], government support [8], digital divide [9] and low usability of the government websites. Another important factor in the adoption of new technologies required in electronic government is trust in the government. Communication with citizens has been recognized as the most important measure to build this trust towards electronic governance [10-13]. The four main potential strengths of social networks. They are collaboration, participation, empowerment and time. These facilitate governments to serve their people like them promote information, services and collaboration of governments with their stakeholders that bring together governments Agencies, citizens, work agencies and information. Social media can expand the use of the Internet to make full Benefits of electronic governance. Social networking sites not only it offers benefits to electronic governance through the intensification and monitoring of services, but also reduces costs while improving their quality Using these sites, governments can publish employment Advertising, promotion of services, advertisement and market. events, seek public opinion and cooperation and collaborate through its various geographic agencies. As Social media have a huge prospect to increase citizen use of the electronic service [14] and electronic participation [15], its greater use by the public could increase transparency. which in turn can increase trust in the government. A recent review [16] of the use of social networks in electronic government has He listed his other various applications in e-government. In his recent report entitled "Design of social media Government policy: Eight essential elements" [17] The Center has identified three different ways of using social networking sites by employees at work Technology in Government, University of Albany. These uses are for the official interests of the agency, professional interests and personal interests. Often, these three are not mutually exclusive and sometimes there are no clear lines dividing the use of the official agency of professional use or Professional use for personal use. David Landsbergen In his recent research work [18,19] he identified ways in which what social media tools are used in different government agencies and five mechanisms were collected as shown In **Figure 1**, the tools of social media can be done by the Government 2.0.

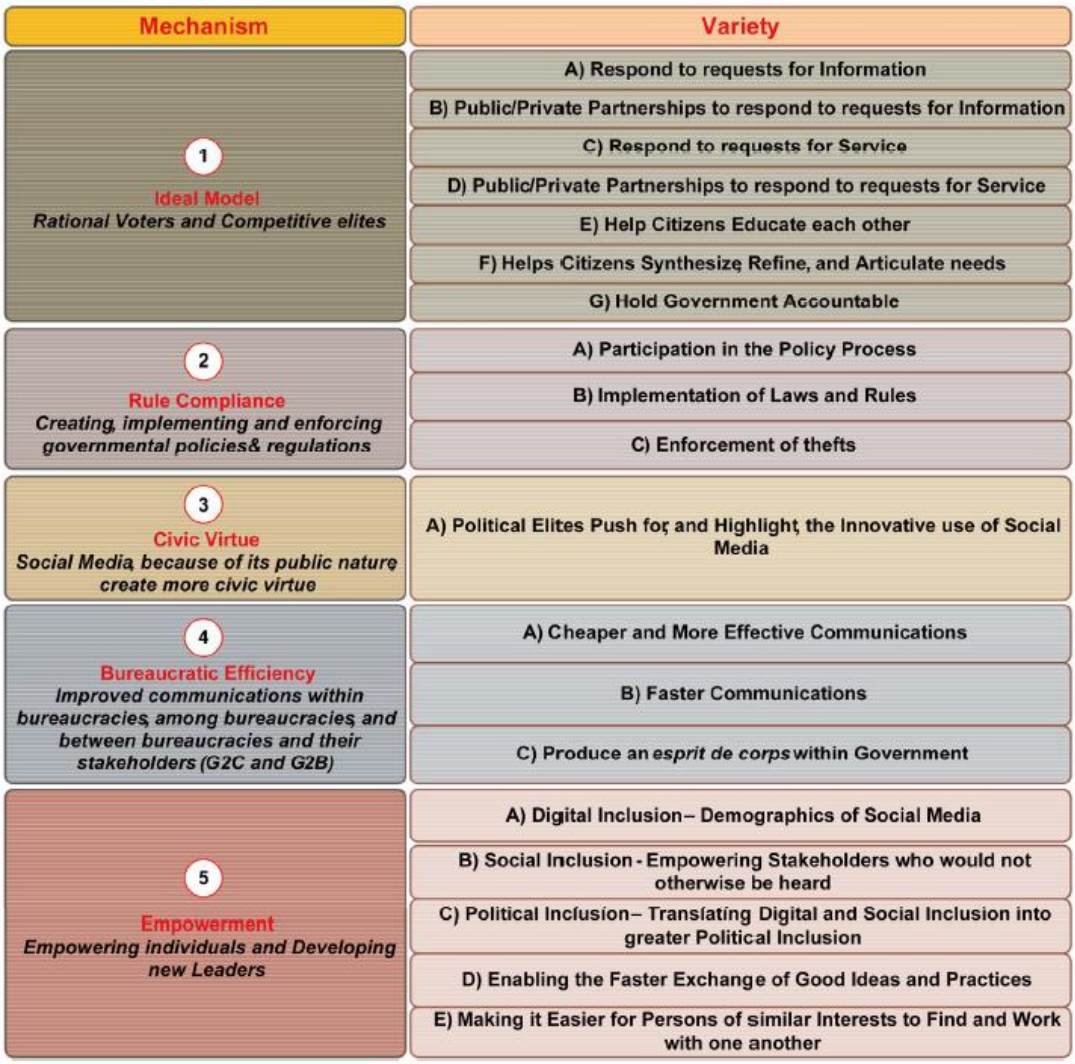

Figure 1. Mechanisms by which social media tools can realize Government 2.0.

IV. RISKS IN THE USE OF SOCIAL MEDIA FOR E-GOVERNANCE

Government information systems that include their infrastructure, individuals, agency, employees and information face persistent, widespread and aggressive threats [20]. This situation is intensified by the environment created by social networks because it uses Web 2.0 technologies that constantly change and involve risks on multiple fronts, including those related to behaviour, ergonomic configuration, regulation and technology [21]. As the risks involved are interdependent, therefore, one can intensify the other. Since the Web 2.0 environment gives its users immense power to collaborate, share and interact, they can easily perform practices that could infringe the rights of others. The most common risks related to user behaviour during interactions on the Web are risks to reputation, privacy, intellectual property and the publication of personal and illegal content. Social networks have the potential to increase campaigns for or against governments or groups. There has also been a sinister use of social networking tools, for example, during the riots of the summer of 2011 in the United Kingdom. In Kashmir, the 2011 increase in the separatist movement that caused riots in Kashmir was also directly influenced by the use of social networks. Technological advances on the Web have created interfaces and services that are easy to use and easy to use. Web 2.0, including social networks, now provides easy environments for sharing documents, videos and audio, creating groups, adding friends online, publishing profiles, etc. Some configurations also allow this work to be done anonymously. This flexibility in configuration can risk its users to inadvertently violate privacy, intellectual property and other regulations or take actions that may be illegal. Social media allows its users to create their detailed profiles, which include personal information, relationships, images, etc. that

can be seen by others and then reorganized and transformed into unacceptable formats and platforms. Governments and organizations have created laws and regulations that describe what is "right" and what is "wrong" when they communicate online. Legal frameworks vary considerably from one country to another, but social networks have a global character. In many cases, appropriate punishments are established for the violation of these laws. As Web 2.0 is changing rapidly, therefore, legal frameworks must be updated frequently to address these new developments. However, given that in the social media environment different stakeholders share different positions and play changing roles, it can be difficult to establish responsibility. In addition, with little or no knowledge of the laws governing the use of social media and the consequences for violating some of these laws, users can easily get caught in crimes for having committed crimes and online crimes. Attacks through techniques such as spear phishing, social engineering and web applications for social media risk individuals, agencies, employees and information. When using social networks with little or moderate computing capacity, individuals or employees face multiple risks of highly qualified cyber attacks to engage in illegal activities and commit to the security and privacy of information.

V. SOCIAL MEDIA POLICY AND GUIDELINES FOR E-GOVERNANCE

Social media tools have created opportunities for governments to collaborate and have the potential to help governments reach their citizens, to shape online e-participation and debates, to empower citizens, groups and communities and even to reactivate or demand democracy, and thus take the evolution of electronic government in new directions. Social media applications also present several risks, including isolation, exclusion, violation of privacy, misuse of information and security threats. Therefore, a comprehensive policy framework can serve as a key enabler for government organizations to provide guidelines for the use of social networks in the governess. In the design of policies for the use of social networks in e-government, there are unique challenges, since ambiguity becomes very important in several key parameters, including the expected benefits, the risks involved, effectiveness, etc. Therefore, many government departments around the world have designed guidelines and policies for the use of social networks in electronic governance projects that differ mainly in the elements covered in these documents and the magnitude of the details in each element. Below are the highlights of a detailed analysis [21] in terms of the content and focus of 26 of these documents and a limited survey of the use of social media tools by 32 government professionals:

• Eight fundamental elements for a policy of social media: Employee Access, account management, acceptable use, employee behaviour, content, security, Legal issues and citizen behaviour.

• Only five documents addressed the issue of employee access to social networking sites, most of them suggesting that employee access be controlled by granting access to selected sites only after the justification of the business case.

•Twelve documents addressed the issue of account management, of which eight were from local governments that provided an explicit policy for account management and others were state policies that offered business-level suggestions that varied considerably among themselves.

• Twelve documents addressed the issue of acceptable use particularly for personal use. The guidelines mainly focused on the use of the existing acceptable use policy with regard to ICT infrastructure. It is clear that policy makers strive to draw the boundaries between the personal and professional use of employees.

• Twenty-one documents establish guidelines for employees address the problem of employee behavior, which mostly directly or indirectly refers to the general code of conduct for employees pre-established. Some provided guidelines specifically for social media, including guidelines for respecting headquarters rules, respecting transparency and openness in interactions and trust. No policy document directly recommended sanctions for hosting or disseminating inappropriate or illegal content.

• Fourteen documents addressed the issues related to the content and its management by providing different guidelines in this regard. Some only allow public information officers or selected individuals or agency officials to publish content, while others allow all employees to post information on agency blogs. No policy provides content guidelines for professional or personal use. Ten policy documents contain instructions to provide a standard disclaimer to announce that the opinion and content of employees may not coincide with the position of the agency.

• Fifteen documents provided one or more specific guidelines, mainly technical and behavioural to ensure data security and the technical infrastructure of the agency. Some pointed to the use of the existing IT security policy. Several concerns related to the technology guidelines addressed in these policies included password security, functionality, the use of public key infrastructure for authentication, virus scanning, the use of complex passwords, the restriction for the publication of classified information and control of account credentials. The concerns addressed in some documents included phishing, social engineering, publication of classified information and citizens.

• Some of the documents specifically pointed to existing laws and, on the contrary, others took an approach suggesting employees to adhere to existing ones Laws and regulations without pointing to the real. The laws mentioned explicitly refer to privacy, freedom of expression, freedom of information, Management of public records, public disclosure

and accessibility. Some address potential legal issues by directing the use of liability waivers in various ways on social networking sites.
Eleven documents addressed in question of citizen behaviour mainly by providing guidelines to deal with Comments posted by citizens. Some allow the publication of Comments from citizens, while others do not. Those that allow the publication of comments provide rules that refer to offensive language, incitement to violence, or promotion, illegal activities among these, some suggest designating the responsibility for controlled flow and moderation of comments.

VI. ESSENTIAL CORE ELEMENTS OF A SOCIAL MEDIA POLICY STYLING

The central elements of a social networking policy as identified in [17] are shown in **Figure 2**. Each of the elements covers a set of issues that must be addressed adequately in any successful social network policy for government agencies. Below, these central elements and the problems in each one are briefly detailed: Employee access: at work, employees can use social network sites in order to carry out commercial or professional development activities or any other interest personal. Access to social networking sites can be controlled by different forms of filtering. Control of access to social networking sites of different types of employees who perform different roles in an organization is fundamental to the effectiveness of e-government. Employee access to social networking sites can be controlled by limiting it to some number or type of employees or limiting the sites or both. Account management: the management of accounts in an agency must not only keep a record of social network accounts created, maintained and closed by their employees for work or professional use, but also to define the procedures for the creation of such accounts. The account management policy for use in a government agency must clearly defined as an account that gives access to all the functions of that social networking site. An official account can be granted on a social media site through the approval of a designated official or through the approval of more than one designated official.
Employee access: at work, employees can use social networking sites in order to carry out commercial or professional development activities or any personal interest. Access to social networking sites can be controlled by different forms of filtering. Control of access to social media sites by different types of employees who perform different functions in an organization is fundamental to the effectiveness of electronic administration. Employee access to social networking sites can be controlled by limiting it to some number or type of employees or by limiting the sites or both.

Account management: the management of accounts in an agency is not only required to keep a record of social media accounts created, maintained and closed by their employees for work or professional use, but also to define the procedures for the creation of those accounts. The account management policy for use in a government agency should be clearly defined as an account that gives access to all functions of that social media site. An official account on a social networking site may be granted by the approval of a designated official or by the approval of more than one designated official.

Acceptable use: the acceptable use policy governs not only the use of social networks but also the use of Internet and other technologies by employees. Can, quantify hours online, monitoring usage, penalties for policy violation, etc.

Employee conduct: The employee's conduct policy governs, Ethics, behaviour and online penalties for employees for violating this policy. The general code of conduct of employees within a government agency to differentiate between "right" and "wrong" in terms of employee behaviour may not cover new problems associated with social media. Therefore, the code of political conduct for employees. The social networks that govern must be reviewed periodically to cover new topics.

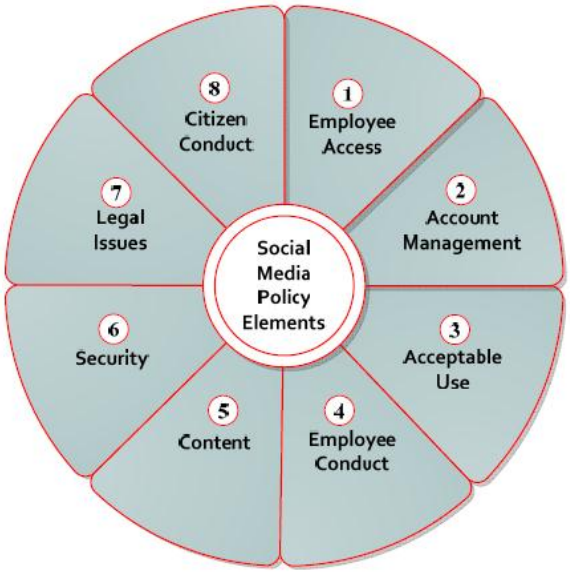

Figure 2. Eight essential core elements of a social media policy

Content: the content policy controls permission for employees to post and manage content on the official social media pages. It should also regulate what type of official content can be published on the personal or professional social networks page of employees.
Security: security guidelines aim to safeguard government data and the technical infrastructure associated with the use of social networks for technological and behavioural risks. Social media, when used in electronic administration, involves new security and privacy issues that a successful policy must address adequately.

Legal Issues: Legal guidelines ensure that government employees comply with existing laws and regulations when using social media tools. In recent years, governments have enacted laws that regulate the use of information technology by individuals and organizations. However, social media has created possibilities for unique technological, behavioural and social crimes that may not be covered directly by existing laws, therefore, existing laws related to information technology must be constantly increased to control new ones crimes.

Citizen conduct: Given that the integration of social networks with electronic government makes it possible to have a public communication between the government and the citizenry, therefore, the rules are created for the commitment of the citizenship with the government. These rules govern various aspects of opinions and comments, whether or not they allow comments and opinions, sanctions for the use of offensive language, incite violence and promote illegal activities.

VII. INDIAN GOVERNMENT FRAMEWORK & GUIDELINES FOR USE OF SOCIAL MEDIA IN E-GOVERNANCE

In India, various policies / frameworks, standards, guidelines and best practices for e-governance have been devised and various committees such as Metadata and Data Standards (MDDS), Biometrics, Localization, Security, Mobile Governance, Interoperability Framework E- Governance in India (IFEG), digital signature, etc. they have been constituted to formulate standards. In September 2011, government. of India formulated a draft framework and guidelines that were updated in April 2012 for the use of social networks for government organizations [22]. The guidelines are intended to help the e-government projects of central and state governments that are implemented within the framework of the national e-governance plan for the participation of social networks in these projects. The document briefly presents social networks, their need in government agencies, in addition to providing a framework and guidelines for their use. The framework is composed of seven elements that group several topics related to the use of social networking sites. Some of the problems are highlighted only while others provide detailed guidelines in this document. These important elements and problems in each of the elements are shown in **Figure 3**. The following sections briefly present several highlights of this framework:

- The framework consists of seven stages that represent seven elements connected in a cycle to demonstrate the continuous evolution and scope of the improvement. Some problems have been addressed in multiple stages.
- Government agencies can use social media for the dissemination of information or for public commitment. These include its use for policy making, education and hiring.
- Government agencies can use existing social media platforms, such as social networks, social bookmarking, desktop publishing, transaction guidance or any other similar means. Agencies can also create their own social communication platforms provided that existing laws permit and considering the duration, type and scope of the public commitment that it is intended to offer.
- The official pages in the social networks must reflect the official position and the interaction must comply with the rules and comply with the existing laws regarding the management of accounts, answers, use of resources, roles and responsibilities, responsibility, creation of content, accessibility and moderation Records management, data security and privacy and employee identity.
- A government agency must maintain the same meaningful name in different social networking sites (as much as possible) and an adequate record of login IDs and passwords. However, the commitment of the employees can be through personal or official accounts, but official responses must be brief and to the point through non-anonymous official accounts and by the official identified only within the predetermined response time. Mail integration can be used to ensure a timely response. In the event that an employee posts comments in a personal capacity, it must be ensured that confidential information is not divulged and the commitment clearly states that the comment is personal and not official. Answers to frequently asked questions should be prepared, maintained and displayed, so participation should not be encouraged separately. Social networks should be used for the propagation of only official policies and should not publish unverified information or frivolous material.
- Resources for social networks and their responsibilities can be subcontracted or internal to an agency. For a moderate conversation, it is necessary to have dedicated resources, including a well-trained leader within the agency. Clearly defined roles and responsibilities must be defined with respect to the response to the Right to Information (RTI), the maintenance of IDS and passwords, data security, privacy, etc. The commitment must be governed by the RTI Act, the IT 2000 Act and the IT Amendment Act 2008.

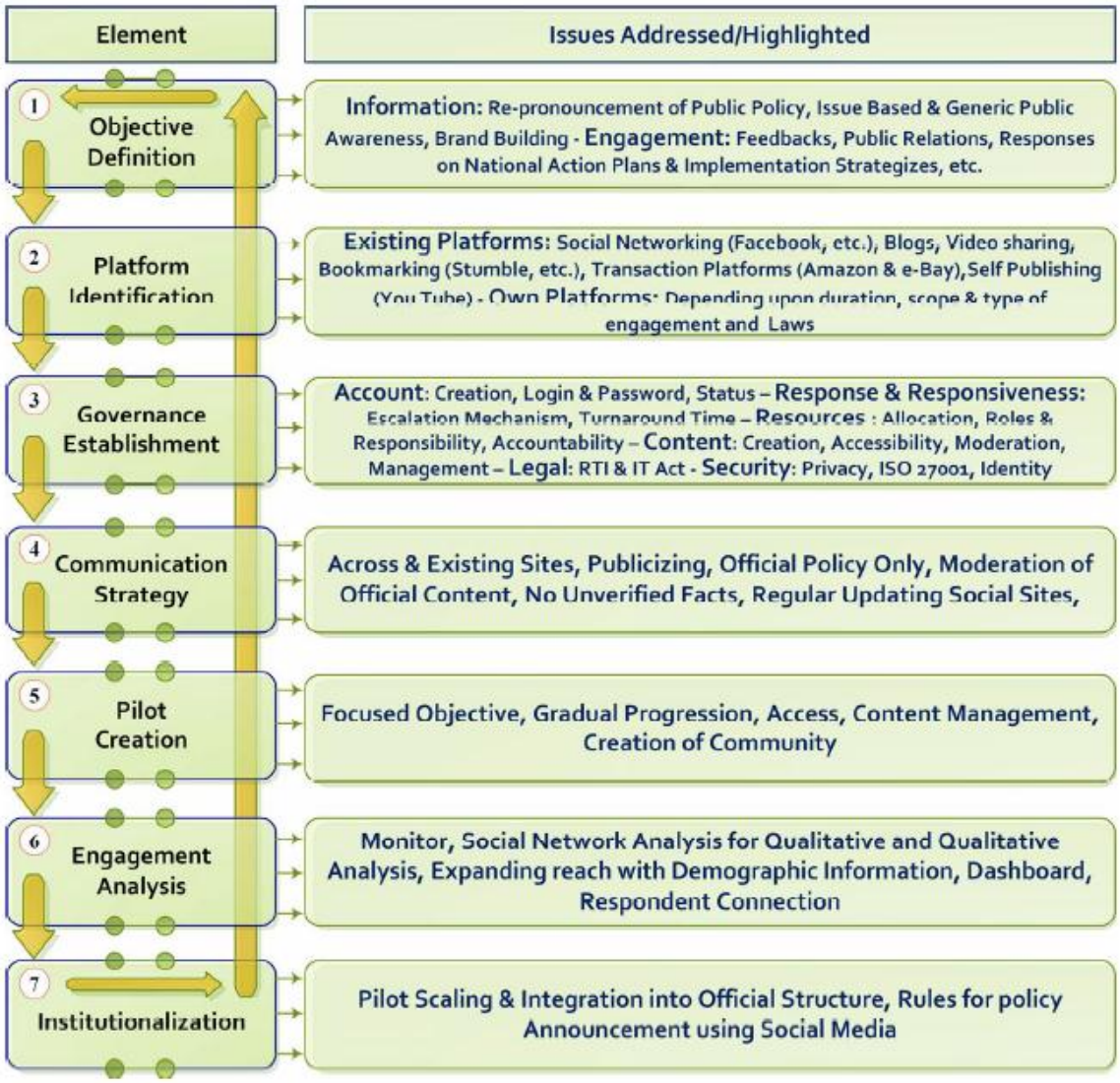

Figure 3. Indian Government framework for social media

• The official content should be specified, adapted, moderate and follow the guidelines of the Government of India for websites, address the challenges related to the accessibility of Indian languages and people with different abilities. The records of interactions that influence decision making should be retained in printed / hard copies. Agencies are encouraged to enter into service level agreements with social media service providers to ensure India's regulations for storage, archiving, access, complaints and response mechanisms.

• All existing laws, most notably the RTI Law, the IT Law 2000 and the IT Amendment Act 2008, govern participation in social networks. The security of personal data is governed by the standards of information technology (reasonable security practices and confidential personal data or information) and ISO 27001. The privacy of individuals must be guaranteed in accordance with the laws in force governing the data protection and privacy.

• A pilot should be created to test the effectiveness and effectiveness of commitment to the public. The commitment must be monitored quantitatively and qualitatively through the analysis of social networks and demographic information, the boards and the connection of the respondent must be used to expand and expand the commitment. After successful completion of the pilot, it must be scaled and fully integrated into the administrative and communications structure of the agencies.

VIII. LIMITATIONS OF INDIAN GOVERNMENT GUIDELINES FOR THE USE OF SOCIAL MEDIA IN E-GOVERNANCE

Although this framework and guidelines have been revised in April 2012 after its initial preparation, there are several problems that have not been fully addressed or have not been included in the guidelines. The deficiencies in the framework are listed below:

- No clear guidelines have been suggested regarding the permission of employees to access social networking sites during office hours for professional and personal use, nor have technological measures such as filtering been suggested to control employee access to these sites in the frame. The purpose of the use of social networks in government organizations does not include the use of social networks for the professional and personal development of employees. In addition, the guidelines do not include instructions on the mechanism for granting controlled access (justification of business cases, access to selected sites, duration of access, etc.) to employees of social media sites for official purposes.
- Although the management of the account has been covered by the guidelines, certain problems have not been discussed, such as the procedure for granting permission to an official to obtain an official account on the social networking site. A public information officer in most such policies is in charge of granting such permission. For strict control, the approval of two parties, such as the communication department and the IT department, has often been suggested.
- The subsection of policy governance of the policy covers acceptable use that does not directly quantify online hours, usage monitoring, penalties for policy violations, etc. However, it suggests that the authorized employee to interact with the public should be held accountable and points out the existing immunity provision of the RTI Act, the IT Law and the IT Amendment Act 2008. In addition, as some other policies and documents, has not drawn limits between the personal and professional use of employees.
- Guidelines for employee behaviour have been given in multiple places in the document that are in tune with those guidelines provided in other policy documents. Detailed guidelines have been provided for the legal provisions in this regard. Given that social media provides an opportunity for participation 24 hours a day, 7 days a week, the guidelines are not sufficient to address the behaviour of employees from professional and personal accounts.
- The guidelines for employees to publish in a personal or professional capacity have not been addressed in the framework. The guidelines do mention the content moderation requirement; however, it does not provide sufficient guidelines to set responsibilities within the organization for this purpose. Various policies allow their employee to post freely on the agency blogs on various mission related topics but Indian guide lines are silent in this regard.
- The framework has provided guidelines for security of personal data and also has covered privacy of individual; however, it lacks technical guidelines for achieving the same. No guidelines have been pro- vided for password security, functionality, use of PKI for authentication, virus scans, use of complex passwords, and control of account credentials. It does not provide guidelines for spear phishing or social engineering.

- Legal guidelines have been provided at multiple places in the framework, however, the laws that include RTI Act, IT Act, and IT Amendment Act 2008. Though, most of the issues are covered by these laws but social media has created possibilities for unique technological, behaviour, and social crimes which may not be directly covered by these laws, therefore, existing Information Technology related laws need to be constantly augmented to check new crimes.

- With respect to the citizen conduct, rules have been clearly depicting how to a government agency should classify comments and engage with the citizens. They specify who and when is necessary and not necessary to respond to comments. Further, they also specify why and how comments that make influence on the policy making decision should be preserved. However, the policy is silent about mechanism that could make a public comment or feedback acceptable or not for the purpose of policy making, etc.

- The guidelines are silent about information confidentiality, integrity and availability and procedures government agencies should adopt this trio. Though the policy refers to the adherence to various sections of IT Act 2000 and its amendment but no reference has been given to any information standard act. ICT faces severe security challenges but no specific or very limited guidelines are provided for information security education.

- The guidelines fall short to address risk management, mitigation and issue of acceptance of residual risks by the use of social media. Though the guidelines en-courage agencies to enact service level agreements with operators of social media sites but do not provide guidelines about what agencies should the organization for this purpose. Several policies allow your employees to publish freely on the agency's blogs on various mission-related topics, but the Indian guides are silent about it.

- The framework has provided guidelines for the security of personal data and has also covered the privacy of individuals, however, lacks technical guidelines to achieve

the same. No guidelines have been provided for password security, functionality, use of PKI for authentication, virus scans, and use of complex passwords and control of account credentials. It does not provide guidelines for phishing or social engineering.

- However, legal guidelines have been provided in various parts of the framework; however, they all repeat the existing laws that include the RTI Act, the IT Law and the IT Amendment Act 2008. However, most of the problems are covered by these laws, but social networks did create possibilities for unique technological, behavioural and social crimes that may not be covered directly under these laws, therefore, existing laws related to information technology must be constantly increased to control new crimes.

- With respect to citizens' behaviour, the rules have clearly described how a government agency should classify comments and engage with citizens. They specify who and when is necessary and not necessary to respond to comments. In addition, they also specify why and how the comments that influence the decision-making of political decisions should be preserved. However, the policy does not say anything about the mechanism that could make a public comment or feedback acceptable or not for the purpose of formulating policies, etc.

- The guidelines do not mention the confidentiality, integrity and availability of information, and the procedures that government agencies must adopt to achieve this trio. Although the policy refers to the adherence to several sections of the IT Law 2000 and its amendment, no direct reference to any information security act or rule has been given. ICTs face serious security challenges, but specific or very limited guidelines for information security education are not provided.

- The guidelines fall short to address risk management, mitigation and the problem of accepting residual risks through the use of social networks. Although the guidelines encourage agencies to enact service level agreements with operators of social networking sites, they do not provide guidance on what agencies should look for these operators with respect to stronger security and privacy controls, multi-factor authentication, cross-site scripts, persistent Cookies, moderation and content monitoring, access to the official accounts of employees and validation and signing of codes.

- The guideline does not provide emphasis on periodic awareness and training of safety, policies and best practices for social networks. In addition, it does not instruct agencies to periodically and constantly update their social media policy, especially with regard to privacy and security, content filtering and acceptable use.

IX. RECOMMENDATIONS FOR IMPROVEMENT

The Web 2.0 Security Working Group (W20SWG) responsible for accessing the information security issues surrounding Web 2.0 technologies in the US Federal Government. UU He has provided Guidelines and recommendations for the use of social media technologies in a way that minimizes risks involved in it [20]. The document encourages the use of social networks in government agencies in a solid business case and following appropriate safety guidelines. The recommendations include five categories of controls grouped into technical and non-technical controls. The technical controls are network and host controls and the non-technical controls are policy controls, acquisition controls and specialized training. These security controls must be adapted appropriately so that the integration of social media in electronic governance will be safe.

X. CONCLUSION

The advantages of social media such as collaboration, participation and empowerment have attracted governments to use it in government to gather agencies, citizens, work and agency information. It is used to promote electronic services, increase transparency and improve trust in government. Government information systems face persistent, widespread and aggressive tendencies that are intensified through the environment created by social media, since it involves risks on multiple fronts, including those related to behaviour, ergonomic configuration, regulation and technology. When used in electronic administration, social networks can also present risks of isolation, exclusion, violation of privacy, misuse of information and security threats. Therefore, governments have devised comprehensive frameworks, policies, guidelines and best practices to serve as key enablers for government organizations for the use of social networks in the governess. The different policies emphasize different elements and aim mainly at adhering to existing laws and regulations to ensure data and information. Some policies suggest that the decision to incorporate social networks into e-government in an agency must be supported by strong business justifications but with adequate security and privacy controls, while others consider that it is necessary for inclusion or do not provide adequate guidance . Security lines and data privacy. The framework of the Indian government is in tune with other similar policies and also includes policies for its multilingual culture. However, it does not include guidelines for all the central elements identified or does not provide sufficient guidelines for some of the parameters that a successful social networking policy must have. There is room for improvement in each element included in this framework, which is more important in the guidelines regarding security

controls, the acquisition of third-party services, risk assessment, employee training, account management and the legal aspects.

REFERENCES

[1]. M.T. Banday, M.M. Mattoo *"Scientific Research: Social Networking"* http://dx.doi.org/10.4236/sn.2013.22006 Published Online April 2013 *2013* 2, 47-56 (http://www.scirp.org/journal/sn)

[2]. Human Capital Institute, *"Social Networking in Govern- ment: Opportunities and Challenges,"* 2012. http://www.hci.org/files/field_content_file/SNGovt_SummaryFINAL.pdf

[3]. T. D. Susanto and R. Goodwin, *"Factors Influencing Citi- zen Adoption of SMS-Based e-Government Services," Electronic Journal of E-Government*, Vol. 8, No. 1, 2010, pp. 55-71.

[4]. United Nations, *"e-Government Survey,"* 2012. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf. ISBN: 978-92-1-123190-8

[5]. R. Reffat, "Developing a Successful e-Government," Work- ing Paper, School of Architecture, Design Science and Planning, University of Sydney, Sydney, 2003.

[6]. Z. Fang, *"e-Government in Digital Era: Concept, Practice and Development,"* International Journal of the Com- puter, the Internet and Information, Vol. 10, No. 2, 2002, pp. 1-22.

[7]. W. Darrell, *"US State and Federal e-Government Full Report,"* 2002. http://www. insidepolitics.org/egovt02us.pdf

[8]. N. Sampson, *"Bank Marketing International: Simplifying in (Form)ation,"* 2002. http://www.mandoforms.com/news/coverage/bankmarketing.html

[9]. A. Kurunananda and V. Weerakkody, *"e-Government Im- plementation in Sri Lanka: Lessons from the UK,"* Pro- ceedings of 8th International Information Technology Conference, Colombo, 12-13 October 2006, pp. 53-65.

[10]. F. Bélanger and L. Carter, *"The Effects of the Digital Divide on e-Government: An Empirical Evaluation,"* Pro- ceedings of the 39th Hawaii International Conference on System Sciences, Vol. 4, 2006, pp. 1-7.

[11]. D. H. McKnight and N. L. Chervany, *"What Trust Means in e-Commerce Customer Relationships: An Interdisci- plinary Conceptual Typology,"* International Journal of Electronic Commerce, Vol. 6, No. 2, 2001-2002, pp. 35- 59.

[12]. F. V. Morgeson, D. Van Amburg and S. Mithas, *"Mis- placed Trust? Exploring the Structure of the e-Govern- ment-Citizen Trust Relationship,"* Journal of Public Ad- ministration Research and Theory, 2010. http://www.terpconnect.umd.edu/~smithas/papers/morgesonetal2010jpart.pdf

[13]. T. S. H. Teo, S. C. Srivastava and L. Jiang, *"Trust and Electronic Government Success: An Empirical Study*," Journal of Management Information Systems, Vol. 25, No. 3, 2008-2009, pp. 99-132.

[14]. E. W. Welch, C. C. Hinnant and M. J. Moon, *"Linking Citizen's Satisfaction with e-Government and Trust in Government,"* Journal of Public Administration Research and Theory, Vol. 15, No. 3, 2005, pp. 371-391. doi:10.1093/jopart/mui021

[15]. B. Shah, *"Increasing e-Government Adoption through Social Media: A Case of Nepal,"* Örebro University, Swedish Business School at Örebro University, Örebro, Sweden, 2010. http://oru.diva-portal.org/smash/get/diva2:372485/FULLTEXT01

[16]. Y. Charalabidis and E. Loukis, *"Transforming Government Agencies' Approach to e-Participation through Efficient Exploitation of Social Media,"* ECIS 2011 Proceedings, Paper 84, 2011. http://aisel.aisnet.org/ecis 2011/84.

[17]. J. Michael Magro, *"A Review of Social Media Use in e-Government,"* Administrative Science, Vol. 2, No. 2, 2012, pp. 148-161. doi:10.3390/admsci2020148

[18]. J. Hrdinova, N. Helbig and C. S. Peters, *"Designing So cial Media Policy for Government: Eight Essential Ele- ments,"* Center for Technology in Government, University at Albany, 2010. www.ctg.Albany.edu

[19]. D. Landsbergen, *"Government as Part of the Revolution Using Social Media to Open Government,"* Ohio State University, Columbus, 2010.

[20]. D. Landsbergen, *"Government as Part of the Revolution: Using Social Media to Achieve Public Goals," Electronic Journal of e-Government*, Vol. 8, No. 2, 2010, pp. 135- 147.

[21]. C. I. O. Council, *"Guidelines for Secure Use of Social Media by Federal Departments and Agencies,"* Federal CIO Council ISIMC NISSC Web 2.0 Security Working Group, 2009, pp. 1-19.

[22]. P. Trudel, *"Web 2.0 Regulation: A Risk Management Process,"* Canadian Journal of Law and Technology, Vol. 7, No. 2, 2010, pp. 243-265. http://cjlt.dal.ca/vol7_ no2/pdf/trudel.pdf

[23]. DEIT, *"Framework & Guidelines for Use of Social Media for Government Organizations,"* Department of Electron- ics and Information Technology, Government Of india, 2012. http:// www. negp. gov. in / pdfs / Social % 20Media%20Framework%20and%20Guidelines.pdf

[24]. Nilamadhab Mishra , "*Internet of Everything Advancement Study in Data Science and Knowledge Analytic Streams*", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.1, pp.30-36, 2018

Authors Profile

Mr. Mahammad Idrish I. Sandhi pursed Bachelor of Computer Application (BCA) from Hemchandracharya North Gujarat University, Patan in 2005 and Master of Computer Application (MCA) from Hemchandracharya North Gujarat University, Patan in year 2008. He is currently pursuing Ph.D. and currently working as Assistant Professor & Head in Department of Computer Application (MCA), Sankalchand Patel College of Engineering, Sankalchand Patel University,Visnagar since 2008.He has published more than 05 research papers in reputed international journals and conferences and it's also available online. His main research work focuses on Big Data Analytics, Social Media, Data Mining and IoT. He has 11 years of teaching experience and 5 years of Research Experience.

Dr. Dilendra Hiran pursed Ph.D in Computer Science from Pacific University, Udaipur in 2015. He completed his Master of Science in Mathematics and Computer Sceince in 1999. Bachelor of Science in Mathematics from MLSU, Udaipur in 1994. He is currently working as Principal, Faculty of Computer Application, Pacific University, Udaipur.

Dr. Nimesh I. Modi pursed Ph.D in Computer Science in from Hemchandracharya North Gujarat University, Patan in 2012. He pursued his Bachelor of Science in Chemistry from Hemchandracharya North Gujarat University, Patan in in 1994. He has pursued his Post Graduate Diploma in Computer Applcation from from Hemchandracharya North Gujarat University, Patan in 1997. He has completed his Master of Business Administarion(MBA) in from Hemchandracharya North Gujarat University, Patan in 2000. He is currently working as Assistant Professor & i/c Head in Department of Computer Science, Hemchandracharya North Gujarat University, Patan. He has 15 years of teaching experience and 10 years of Research Experience.

