Prevention of cybercrimes in smart cities of India: From citizens' perspective

Sheshadri Chatterjee
Department of Management Studies
Indian Institute of Technology Delhi
Email: sheshadri.academic@gmail.com

Arpan Kumar Kar
Department of Management Studies
Indian Institute of Technology Delhi
Email: arpan_kar@yahoo.co.in

Yogesh K. Dwivedi (**Corresponding author**)
Emerging Markets Research Centre (EMaRC),
School of Management, Swansea University Bay Campus,
FabianWay, Swansea SA1 8EN, Wales, UK
Email: y.k.dwivedi@swansea.ac.uk

Hatice Kizgin
Emerging Markets Research Centre (EMaRC),
School of Management, Swansea University Bay Campus,
FabianWay, Swansea SA1 8EN, Wales, UK
Email: Hatice.Kizgin@Swansea.ac.uk

Abstract

Purpose –The purpose of the study is to identify the factors influencing the citizens of India to prevent cybercrimes in proposed Smart Cities of India.

Design/methodology/approach –A conceptual model has been developed for identifying factors preventing cybercrimes. The conceptual model was validated empirically with a sample size of 315 participants from India. Data was analysed using Structural Equation Modeling with SPSS and AMOS software.

Findings –The study reveals that 'awareness of cybercrimes' influences significantly towards actual usage of technology to prevent cybercrimes in Smart Cities of India. The study reveals that government initiative and legal awareness have less impact towards spreading of awareness of cybercrimes to the citizens of proposed smart cities.

Theoretical implications – The conceptual model utilises two constructs from technology adoption model namely perceived usefulness and ease of use. The study employs other factors such as, social media, word of mouth, government initiatives, legal awareness and organisations constituting entities spreading awareness from different related literature. Thereby a

comprehensive theoretical conceptual model has been proposed which helps to identify the factors that may help in preventing cybercrimes.

Practical implications –This study provides an insight to the policy maker to understand several factors influencing the awareness of cybercrimes of the citizens of proposed Smart Cities of India for prevention of cybercrimes.

Originality/value – There are few existing studies analysing the effect of awareness of citizens to mitigate cybercrimes. Thus, this study offers a novel contribution.

Keywords –Cyber security, Digital services, ICT4D, Smart City, Social engineering.

Paper type –Research Paper

1. Introduction

The internet has emerged as an important infrastructure in our daily life in this journey towards digital transformation (Castiglione *et al*., 2018). In this journey, the Government of India (GoI) has announced the intension to create 100 smart cities in India (SCI). Smart Cities are construed to be datafied or internet cities (Gosgerove, 2011; Falconer, 2012; Gupta, 2014; and Chatterjee, & Kar, 2017). The GoI is developing the SCI concept with a core of information communication technology (ICT activity). However, there are concerns that the SCI concept might be adversely affected by security problems (Thomson, Von Solms, & Lauw, 2006; Chaturvedi, Sing, Gupta, & Bhattacharya, 2014; Dwivedi *et al*., 2017; Gcaza, Solms, Grobler, & Vuuren, 2017). It is expected that citizens of SCI would use high-speed internet for ensuring easy access to digital services (Chatterjee, & Kar, 2017; Chhonker, Verma, & Kar, 2017). As a result, this vulnerability might be increased. So, it is necessary to identify the perceived security determinants necessary for ensuring cybersecurity. The perceived security may affect adoption and usage of IT services in SCI. Also, with the increase of ICT, the number of cybercrimes might be increased. Cybercrimes may be defined as "Criminal activity directly related to the use of computers, especially illegal trespass into the computer system or database of other, manipulation of theft of stored or on-line data, or sabotage of equipment and data" (Om pal *et al*., 2017, p. 166).

In India, the commission of cybercrimes is posing an increasing threat especially for the citizens of SCI that require prevention. Now, before discussing preventive measures of cybercrimes in SCI, it is important to realize the conception of Smart City (SC). We can designate a city to be 'Smart' if the city has the capability of balancing social, economic and environmental developments in a sustainable way and if, with the help of government, the city can link-up all democratic processes effectively (Caragliu, Del Bo, & Nijkamp, 2011). The smart city authorities are expected to provide digital services to the citizens taking help of innovative technologies. These digital services would be available to the citizens for different sectors like

smart transport, digital health care, smart energy, e-education and even IoT technology (Chatterjee, Kar, & Gupta, 2018). The use of ICT is essential to ensure balance among these developments (Tryfones, Kiountouzis, & Poulymenakou, 2001). The government is required to engage citizens effectively with modern technologies to improve society and their lived experience (Kickbusch, & Gleicher, 2014). Realizing the fact that a country can leverage its national wealth through adoption of modern technologies, the developed countries of the world have already done the needful to expedite production of goods and services. They have created smart cities to improve the living standard of the inhabitants (Comin, & Hpboijn, 2008; Foster, & Rosenzweigh, 2010; Chatterjee, & Kar, 2015).

The principal categories of cybercrimes are, for example, Cybercrimes against society, cybercrimes against property, cybercrimes against individuals and cybercrimes against organisations (Brenner, & Goodman, 2002). Now to combat the cybercrimes inimical for progress and developments of SCI, the citizens' awareness regarding cybercrimes is very much instrumental (Muniandy, & Muniandy, 2012). As the sense of awareness regarding cybercrimes grows, the citizens of SCI would become cautious regarding the menace of cybercrimes. Hence, this act of social engineering for developing awareness is a crucial issue (Mehta & Singh, 2013). Typical cybercrimes against society include currency forgery, cyberterrorism, illegal website amendments, revenue stamp forgery etc. (Sproles, & Byars, 1998). Cybercrimes against property include credit or debit card fraud, infringement of Intellectual Property Rights (IPR) with software piracy, infringement of copyright, theft of coding, trademark breach and so on (Supriya, 2012). Cyberbullying, cyberdefamation, cyberstalking, email spoofing, hacking, spamming, (Parthasarathi, 2003, Joshi, 2016) and so on come under category of cybercrimes against individuals. Cybercrimes against organisations include data theft of organisations, email bombing, infringement of trade secret using cyberspace, logic bomb, unauthorized access to computers, virus attack and so on (Parthasarathi, 2010; Weerakkaly, Irani, Kapoor, Sivarajah, & Dwivedi, 2017). Cybercrimes are also said as 'Internet Crimes' or 'Computer Crimes' and it includes criminal activities actuated using computers (Kelly, 1999). These have become a great concern for SCI (Mohamed, 2003; Obuh, & Babatope, 2011).

For addressing cybercrime challenges (Zhao, Scavarda, & Waxin, 2012), the citizens are required to use the preventive technologies if they are aware and conversant regarding the usefulness of the technology and if they do not feel difficulties in using the technologies (Davis, 1989). Thus, there comes the question of adoption capabilities of these technologies. Adoption behavior has been studied utilising apposite inputs from other studies (Williams, Dwivedi, Lal, & Schwartz, 2009; Dwivedi, Rana, Janssen, Lal, & Williams, 2017). For this, different adoption behaviors and models have been studied including Technology Acceptance Model (TAM). The inputs derived from these studies have helped to identify the factors responsible to enhance citizens' awareness regarding cybercrimes. It has helped to identify how the citizens of SCI would easily use these preventive technologies. With some recommendations, the study ends with a comprehensive conclusion.

This paper tries to find out the answers of the questions (a) why there is necessity to prevent cybercrime in SCI? (b) what are different entities responsible for spreading awareness among the citizens of SCI regarding menace of cybercrimes? (c) how the actual use of preventive technologies can ensure prevention of cybercrimes in SCI? (d) what are the perceived determinants influencing the citizens to prevent cybercrimes in SCI? (e) can we develop a theoretical model for prevention of cybercrimes in SCI?

In subsequent sections, a detailed review on the background literature is presented followed by a section on how the conceptual theoretical model is developed. This is followed by a description of the research methodology and then the results of our study have been elaborated. This is followed by the discussion on the implication to theorists and practitioners. The article subsequently highlights the limitations with directions of future research. It concludes with the key takeaways for the readers.

2. Literature review

In the subsequent subsections, we explore the relevant existing literature surrounding smart cities, cybercrimes and the regulatory ecosystem surrounding cybercrimes in India.

2.1 Smart Cities of India

In smart cities, there will be appreciable use of digital services by the citizens to perform their daily activities (Carlino, 2011). The citizens of SCI are expected to enjoy digital services including facilities of having smart buildings (Tagliabue, Buzzetti & Arosia, 2012; Gul & Patidar, 2015), advantages of smart water management (Van den Bergh & Viaene, 2015), smart education (Bakry, 2004) and so on. The citizens of SCI are expected to perform their daily commercial activities with the help of e-commerce platform (Alomari, Woods, & Sandhu, 2012; Mansoori, Sarabdeen, & Techane, 2018). These include digital payments, mobile banking and so on. The citizens are expected to use high-speed networks (Chatterjee, Kar & Gupta, 2017).

It is pertinent to mention here that shaping of SCI is still in evolution stage. There is a limited literature considering the context of India regarding issues of cybercrimes in SCI. The citizens of proposed SCI are expected to depend on online platforms for performing their daily activities and hence they are required to be aware and cautious regarding their online activities (Rana, Dwivedi, Williams, & Weerakkody, 2016). In India, it is experienced that most popular social platforms are Twitter, LinkedIn, Facebook and so on though many citizens of SCI are expected to use these platforms simultaneously. Thus, social media would act as an effective factor for the citizens of SCI to improve their awareness regarding cybercrimes as it would be helpful for effective interactions through social media (Zhang, & Benyoucef, 2016). The citizens of SCI are expected to interact directly with each other through Word of Mouth (WoM). It is expected that awareness related to cybercrimes might be increased through this direct interaction. However, WoM could act as a substantial determinant to enhance awareness of cybercrimes for the citizens of SCI. This is because information spread through WoM could motivate the citizens of SCI to realize the consequences of cybercrimes (Chu, & Kim, 2011; Cheung, & Lee, 2012; Cho, Park, & Kim, 2014).

2.2 Cybercrimes in Smart Cities of India

Cybercrime constitutes as an act committed or omitted in contravention of law commanding or forbidding it and for this, there is provision of punishment (Agarwal, 2015). There are diverse types of cybercrimes (Saini, Rao, & Panda, 2012). These are described in Table 1.

Table-1: Various kinds of Cybercrimes

Cybercrimes	Explanation	Reference
Hackers	Out of curiosity or to be involved in competition with their friends or for education or otherwise, some individuals, called Hackers, used to have	Thomas, & Loader, 2000

	explored computer system of others.	
Pranksters	These individuals used to have perpetrated tricks on others, especially not intending to cause any specific or long-lasting damage	Richards, 1999
Crackers	Just for a fun or for causing loss to others with ulterior motive, some individuals create virus. These individuals are called crackers.	Chan, Fan, & Prodromidis, 1999
Cyber terrorists	There exist several types of cyber terrorisms. It is, sometimes, a smart hacker who attempts to break a Government website or it may be a group of identical minded netizens who intend to crash a website with the help of flooding the website with traffic. Apparently, this action appears to be innocent, but it can invite many damages and it is still illegal.	Longstaff, & Schultz, 1993;
Cyber bulls	It is a harassment committed by individuals with the help of internet. Unkind email messages, vicious forum posts, posting fake bio-data on websites and so on come under this category.	Adams, 1996; Chen, Zeng, Atabakhsh, Wyzga, & Schroeder, 2003
Salami attackers	For committing financial crimes, some individuals commit these attacks. The secret here is to make an insignificant charge so that in a particular case none will notice it, for example, an employee of a bank puts a programme in the server of the bank and it goes on deducting small amount from every customer regularly.	Philippsohn, 2001
Career criminals	There are individuals who earn part or all concerning to their income from crimes committed with the help of internet. 'The FBI reported in 1995, that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture'.	Bowen, & Mace, 2009

There are other cybercrimes like data crimes, network crimes, access crimes, virus dissemination related crimes and so on (Jankowitz, 1988; Spafford, 1989; Power, 2001).To develop awareness regarding cybercrimes, the authorities including GoI are required to be more up and doing so that affected citizens of SCI can get appropriate remedies (Belapure, & Godble, 2011; Mohit, 2012; Harpeet Sing, 2015). In the developing countries, it is observed that financial losses incurred by organisations are almost 80% due to computer breaches (Saini *et al*., 2012). Once the awareness of the citizens of SCI is increased by brushing up this psychology of social engineering (Agarwal, 2015), they will be motivated to use modern preventive technologies provided they feel that these will fetch effective result and would not create constraint to use (Davis, 1989). Technology Acceptance Model (TAM) which has been used here is considered as a special case of Theory of Reasoned Action (TRA) (Fishbein, & Ajzen, 1975). The development of effective awareness concerning to realization of menace of cybercrimes may be achieved easily with the help of social media as an effective medium (Kim, & Srivastava, 2007; Parise, & Guinan, 2008; Kaplan, & Haenjein, 2010). Social media act as an effective instrument in this context (Qualman, 2012; Lu, Fan, & Zhou, 2016).

The government should take appropriate initiatives and spread information through electronic and other media to increase awareness of menace of cybercrimes. This would motivate the citizens of SCI to appropriately use technologies necessary to combat cybercrimes (Shareef, Kumar, Kumar, & Dwivedi, 2011; Zuiderwijk, Janssen, & Dwivedi, 2015). The parts to be played by the organisations in different SCI for boosting up awareness of cybercrimes to the citizens of SCI are pivotal (Mitnick, & Simon, 2011). Organisations should always keep them updated, otherwise it would help the criminals to commit any crime in SCI (Abu-Musa, 2008). If

awareness of cybercrimes can be improved among the citizens of SCI, it would effectively help mitigate cybercrimes in SCI (Mehta, & Singh, 2013; Parmer, & Patel, 2016; Zhang, & Benyoucef, 2016).

2.3 Cyber Crime and Regulatory Ecosystem in India

To address cybercrimes in India, GoI has already framed Information Technology Act, 2000 (IT Act, 2000). Some of its provisions have been amended in 2008 to make the act more stringent against cybercriminals. Most of the provisions of IT Act, 2000 since amended are found to be non-bailable and cognizable. Ironically, it has been observed that some of the provisions of this act might be abused by the law enforcement authorities. For example, the provisions were misused in the case of two-girls who were punished wrongly by the law enforcement authorities in Maharashtra, India (Shaheen Dhada & Others, 2012) by the application of section 66A of IT Act 2000. Eventually, that section 66A of IT Act 2000 since amended was struck down as the Supreme Court of India held *inter alia* that this provision is violative of Article 19(2) of the Constitution of India in the Shreya Singhal case (Shreya Singhal v. Union of India, WP No. 167 of 2012, Supreme Court of India). The GoI is required to restructure the laws to see that provisions are not misused by the law enforcement authorities. If these are done, this would also help the citizens of SCI to enhance their awareness of cybercrimes.

The GoI should also make the citizens of SCI aware regarding extent of punishments available for the delinquents (McConnel, 2000). This might motivate the citizens of SCI for taking legal remedies and would motivate them to appropriately use technologies for addressing cybercrimes in SCI (Holsapple, & Lee-Post, 2006). Ironically the individuals committing cybercrimes often escape punishment for want of appropriate evidence. It has thus become a challenge as to how appropriate evidential proofs of computer crimes committed in SCI can be collected to effectively prosecute the cybercriminals (Jiow, 2013).

3. Development of Conceptual Model

We have seen in the background studies that awareness regarding cybercrimes is pivotal for tackling and preventing cybercrimes in SCI (Mehta, & Singh, 2013). Now, we try to find out different entities which could spread awareness of cybercrimes among citizens of proposed SCI. Moreover, while developing the conceptual model, we would try to find out the major factors which might influence actual technology use by the citizens of SCI to prevent cybercrimes.

Without development of awareness regarding menace of cybercrimes, the citizens would not be alert regarding its negative elements (Agarwal, 2015). For this, many agencies are to take initiatives. Government through publicity campaign and by other means can help the citizens to improve their awareness (Gupta, Joshi, & Misra, 2012). In a modern technological environment, social media plays a key role. Everyday activities can be supported through effective use of social media. Through this, accurate information may be obtained by the citizens. Hence, this tool is considered effective to improve awareness (Ellison, 2007; Kim, & Park, 2013). Citizens while interacting with each other, through conversation, can get a scope to develop their awareness regarding the menace of cybercrimes. Hence, WoM is an effective instrument to develop awareness (Hung, & Lai, 2015). In smart cities, many organisations are expected to function. They may be banks, post offices, different financial institutions and so on. These institutions with the help of email, SMS (Short Messaging Services) or otherwise can boost up

the sense of awareness. Hence, role of organisations towards contribution of developing awareness among citizens of SCI count much (Belapure, & Godbole, 2011; Mitnick, & Simon, 2011). If any victim of cybercrime does not get appropriate legal remedy, they will fail to have faith in legal system. Hence, enhancement of legal enforcement towards addressing cybercrimes would increase awareness (Ali, 2011; Michael, Steingruebl, & Smith, 2011). Enhancement of overall awareness of the citizens would help to get them motivated to use the preventive technology. It would also help to prevent cybercrimes (Pevlou, & Fygenson, 2006). Again, if the citizens while using preventive technologies perceive that such use is not fetching useful results, nor the use of technology is free from complexity, they would not be motivated to use that technology (Davis, Bagozzi, & Warshaw, 1989; Park, 2009). Hence, perceived usefulness and ease of use would motivate the citizens to use preventive technology which, in turn, will prevent cybercrimes (Longstaff, & Schultz, 1993; Handerson, & Devett, 2003; Park, 2009).

To visualize, all the factors instrumental to prevent cybercrimes in SCI mediating through two variables, Awareness of Cybercrimes (AOC) and Actual Technology Use (ATU) are shown in the following Table 2. It contains the factors, their corresponding explanations and the respective sources in the form of references.

Table 2: Summary of factors and sources

Factors	Explanation	Source
Government Initiative (GI)	By NISAP (Part of National Cyber Security Policy), by making the citizens of SCI realize regarding needs of prevention of cybercrimes, the GoI should try to improve awareness among the citizens of SCI for prevention of cybercrimes.	Belapure, & Godbole, 2011; Gupta, Joshi, & Misra, 2012; Raghav, 2012
Social Media (SM)	Awareness among citizens of SCI may be developed by Social Media as it would help exchange information regarding menace of cybercrimes in proposed SCI. This ingredient would enhance awareness which in turn motivates the citizens of SCI to actual use of technology to prevent cybercrimes in SCI.	Wolfinbarger, & Gilly, 2001; Devraj, Fan, & Kohli, 2002; Brown, Pope, & Voges, 2003; Pavlou, & Fygenson, 2006; Ellison, 2007; Edelman, 2010; Kim, & Eastin, 2011; Kim, & Park, 2013; Shin, 2013; Yadav, De Valek, Hennig-Thurau, Hoffman, & Spann, 2013; Lu, Fan, & Zhou, 2016; Mikalef, Pappas, & Giannakos, 2016; Zhang, & Benyoucef, 2016; Alalwan, Rana, Dwivedi, & Algharabat, 2017; Alryalat, Rana, Sahu, Dwivedi, & Tajvidi, 2017; Kapoor *et al.*, 2018
Word of Mouth (WOM)	Exchange of views by persons to persons through talks constitute the affairs termed as WOM. It helps to form effective influence to improve awareness of citizens of SCI regarding cybercrimes. It helps developing preventive measure against cybercrimes in SCI.	Chu, & Kim, 2011; Cheung, & Lee, 2012; Wisman, 2013; Zheng, Zhu, & Lin, 2013; Cho, Park, & Kim, 2014; King, Richeria, & Bush, 2014; Hung, & Lai, 2015
Organisations (ORG)	The role of organisations functioning in SCI is vital for forming awareness instrumental to	Abu-Musa, 2008; Gatzlaff, & Mc Cullough, 2010; Belapure, & Godbole,

	prevent cybercrimes in SCI. The functions of the organisations should be flawless to develop trust among the citizens of SCI on these organisations. It would bring confidence of the citizens of SCI over these organisations and in that case the actions of the organisations would impact on the citizens of SCI to develop awareness of cybercrimes.	2011; Mitnick, & Simon, 2011; Harpeet Singh, 2015
Legal Enforcement (LE)	Law Enforcement helps developing awareness among citizens of SCI which in turn would be helpful to prevent cybercrimes. The law enforcing authorities should be effective and efficient to enforce laws effectively.	Mc Connel, 2000; Mohamed, 2003; Burns, Whitworth, & Thompson, 2004; Ali, M.M., 2011; Michael, Steingruebl, & Smith, 2011; Aggarwal, 2015
Awareness of Cybercrimes (AOC)	It is associated with knowledge and attention of the users. This helps the users to know details about internet and its functionalities. This helps the citizens of SCI to improve their awareness of cybercrimes and its dangers. This would help to prevent cybercrimes in SCI.	Aparna, & Chauhan, 2012; Mehta, & Singh, 2013; Avais, & Abdullah, 2014; Singeravelu, & Pillai, 2014; Aggarwal, 2015; Narahari, & Shah, 2016; Parmer, & Patel, 2016
Perceived Usefulness (PU)	It is perception of citizens of SCI for prevention of cybercrimes. It includes many ingredients like effectiveness, performance, trust, risk perception and productivity. It motivates the citizens to actual use of technologies essential to prevent cybercrimes in SCI. It is associated with the sense of perceiving usefulness of the technology.	Davis, 1989; Davis, Bagozzi, & Warshaw, 1989; Handerson, & Devett, 2003; Aggelidis, & Chatzoglou, 2009; Park, 2009; Turner, Kitchenham, Brereton, Charters, & Budgen, 2010
Perceived Ease of Use (PEU)	It is construed to be degree to which citizens of SCI would believe that some efforts are needed to learn for use of a technology essential to prevent cybercrimes in SCI. This ingredient includes factors like simplicity, compatibility, and self-efficacy. This impacts on actual use of technology to prevent cybercrimes in SCI.	Davis, 1989; Davis, Bagozzi, & Warshaw, 1989;Yi, Liao, Huang, & Hwang, 2009
Actual Technology Usage (ATU)	This is related with the conception that users are involved with the use of the technology. This use of technology will help prevent cybercrimes in SCI.	Sorebo, Sorebo, & Sein, 2007;Abdul Nasser, 2012
Prevention of Cybercrimes in SCI (PCS)	The prevention of cybercrimes in SCI includes mechanisms required to increase awareness among the citizens of SCI and includes actual technology use. This would help to prevent cybercrimes in SCI.	Longstaff, & Schultz, 1993; Abdul Nasser, 2012

3.1 Government Initiative (GI): The GoI as well as all state governments are required to take up meaningful initiatives for improving awareness among the citizens of SCI regarding menace of cybercrimes. For this, on 2nd July 2013, the GoI has framed National Cyber Security Policy, 2013 whose principal goal is to build up robust and effective and secured resilient cyberspace for

citizens of SCI (Gupta, Joshi, & Misra, 2012). GoI should take appropriate initiatives to arrange different workshops, conferences, research-based programmes to improve awareness. GoI should promote publicity campaign including seminars, radio and television programmes and so on, National Awareness programmes like National Information Security Awareness Program (NISAP) is to be promoted and to realize cybersecurity requirements for the SCI citizens, effective training and academic programmes are conducted. Government should make the citizens of SCI aware regarding the fact that with more dependence on the internet, they are becoming more vulnerable to disruptions engineered through cyberspace (Gupta, Joshi, & Misra, 2012). Sincere GoI initiatives would improve the awareness of the citizens of SCI concerning to cybercrimes (Belapure, & Godbole, 2011). Besides, the government should take up NISAP to make the citizens of SCI aware regarding menace of cybercrimes (Raghav, 2012). From the above discussions, we can develop the following hypothesis.

H1: Government Initiative (GI) would positively impact on Awareness of Cybercrimes (AOC).

3.2 Social Media (SM): If the citizens of proposed SCI interact among themselves via social media platforms, it would provide more accurate, transparent, and exhaustive information to each other which would enrich their knowledge (Wolfinbarger, & Gilly, 2001; Alryalat, Rana, Sahu, Dwivedi, & Tajvidi, 2017). The interactions among citizens of SCI with the help of social media platform regarding dangers and consequences of cybercrimes would enhance their awareness about cybercrimes. It would enhance their belief that, to prevent cybercrimes in SCI, the citizens are to take recourse to use appropriate technologies (Lu, Fan, & Zhou, 2016; Zhang, & Benyoucef, 2016). The authorities are required to be vigilant to utilize these social platforms to enhance awareness regarding menace of cybercrimes in proposed SCI (Ellison, 2007; Kim, & Park, 2013; Alalwan, Rana, Dwivedi, & Algharabat, 2017). Advancement of technology also would motivate the citizens of SCI to use electronic platforms in a regular way and interactions among the citizens of SCI taking help of social platform would improve the extent of awareness regarding the menace of cybercrimes in SCI (Kim, & Eastin, 2011; Shin, 2013). It is a fact that social media platforms are mainly concerned with affairs of transactions only but at the same time it also acts as an effective instrument for exchange of information through interactions. It would enhance the awareness of the citizens regarding cybercrimes and in turn such awareness would motivate the citizens to use technology to combat cybercrimes in proposed SCI (Devraj, Fan, & Kohli, 2002; Yadav, De Valek, Hennig-Thurau, Hoffman, & Spann, 2013). However, the social media platform is used by SCI citizens in a more efficient way incurring lower costs compared to performing such interactions through traditional media and if used effectively would positively influence the citizens of SCI to appreciably enhance awareness regarding cybercrimes (Edelman, 2010; Mikalef, Pappas, & Giannakos, 2016). Based on the above discussion the following hypothesis is provided.

H2: Social Media (SM) will have positive impact to enhance Awareness of Citizens (AOC) of SCI towards cybercrimes.

3.3 Word of Mouth (WOM): Exchange of views through person to person through WoM discussion acts as a self-leader capable of forming effective opinion among the citizens of SCI (Zheng, Zhu, & Lin, 2013). If persons in SCI speak with each other regarding dangers of cybercrimes, the citizens of SCI would improve their awareness regarding cybercrimes (Hung, & Lai, 2015). WoM is concerned with direct interactions among the citizens. In the context of the

smart city, the direct interaction among the citizens of SCI would come under the remit of WoM. The interactions would be spread and if through any motivation whatsoever one feels the need of enhancement of awareness regrading cybercrimes, their opinion would be spread through WOM among the other citizens of SCI. In that case, it can be said that WoM would help motivate the citizens of SCI to realize the need of improving their Awareness of Cybercrimes (AOC) (Chu, & Kim, 2011; Cho, Park, & Kim, 2014). WoM thus acts as an effective determinant to enhance the extent of awareness regarding cybercrimes. If one of the citizens wishes to spread the boon of possessing AOC, it would be spread by that person through interaction with others in the form of WoM. It would help to enhance the sense of awareness of the citizens of SCI regarding dangers and consequences of cybercrimes (Cheung, & Lee, 2012; Wisman, 2013; King, Richeria, & Bush, 2014). In terms of the above discussions, the following hypothesis is formulated.

H3: Word of Mouth (WOM) has a positive impact over Awareness of Cybercrimes (AOC) among the citizens of SCI.

3.4 Organisations (ORG): To make the citizens of SCI aware regarding menace of cybercrimes, role of organisations is vital (Harpeet Singh, 2015). The organisations in SCI like Banks, Post Offices and other financial institutions play a pivotal role to boost up awareness among the citizens of SCI through their day to day activities. Often, we find messages from the bank authorities cautioning not to disclose bank details to any other persons as it might jeopardize one's commercial interests. Organisations are required to ensure security control and are to report to Indian Computer Emergency Response Team (Cert-in) regarding any security incidence (Belapure, & Godbole, 2011). Besides, organisations' duties are to always keep the concerned beneficiaries appraised regarding any possible future occurrence of cybercrimes. It would help the citizens of SCI to be cautious regarding the occurrence of cybercrimes. They would be aware regarding what to do and what not to do. In this way, organisations contemplated to be working in the SCI should act as an effective instrument to make the citizens of SCI Aware of Cybercrimes (AOC) (Mitnick, & Simon, 2011). The organisations should be constantly seeking to update their internal processes so there would be no future re-occurrence of cybercrime. Such occurrence might adversely affect the citizens of SCI and a sense of lack of trust might grow in that case among the citizens (Abu-Musa, 2008). The organisations should preserve the data of their respective customers, so that there might not be any data breach since in that case, it would bring in adverse conception on the customers (Gatzlaff, & Mccullough, 2010). Thus, there is an effective role of the organisations which would be operating inside the SCI to boost awareness among the citizens regarding menace of cybercrimes. In the light of above discussions, the following hypothesis is prescribed.

H4: Organisations (ORG) have positive impact on the Awareness of Cybercrimes (AOC) among the citizens of SCI.

3.5 Law Enforcement (LE): The very nomenclature 'Law Enforcement' is associated with mechanism instrumental for enforcement of law to address cybercrimes in the present context (Ali, 2011). It is a fact, in many developing countries the laws for tackling the cybercriminals are not strong (McConnel, 2000). In many developing countries, it appears that the authorities are found to invest less amount to enforce laws to address cybercrimes. On the contrary, the authorities are found to invest more amount for enforcement of laws to address other crimes of regular nature (Michael, Steingruebl, & Smith, 2011). For addressing cybercrimes in SCI with the help of proper enforcement of law requires considerable amount of investment. Insufficient investment poses challenges to the law enforcement authorities. This is because, the nature of

cybercrimes is assuming new forms (Mohamed, 2003). It is essential to combat cybercrimes in SCI with the help of enforcement of law (Burns, Whitworth, & Thompson, 2004). In this context, the role of IT authorities is important (Chatterjee, Kar, & Gupta, 2017). The persons using the internet should be aware of the criminal activities occurring in the cyberspace. Online transaction techniques expected to be adopted in SCI would enable massive evolution in the use of the internet as it would change traditional business mechanisms (Ali, 2011). Data and information of the citizens of SCI are supposed to be protected from unauthorized illegal access. One is to know basic information of cyber enactments. Another is to know how those are enforced. Since the laws responsible to book the cybercriminals in India are not so stringent (McConnel, 2000) like other developing countries, the citizens of SCI possess less dependence on these laws. Hence, pragmatic law enforcement against cybercrimes in SCI is essential. Once it is ensured, awareness of the citizens regarding cybercrimes would be increased (Agarwal, 2015). With all these inputs, the following hypothesis is provided.

H5: Legal Enforcement (LE) has a positive impact on the Awareness of Cybercrimes (AOC) of the citizens of SCI.

3.6 Perceived Usefulness (PU): This factor has been taken from the knowledge of Technology Acceptance Model (TAM) (Davis, 1989; Davis, Bagozzi, & Warshaw, 1989). It effectively influences attitudes of the citizens of SCI to use technologies necessary to address and to prevent cybercrimes in SCI. It subsequently impacts on the citizens of SCI for Actual Technology Use (ATU) to prevent cybercrimes. This model basically approached to identify the internal beliefs of citizens of SCI with the help of external variables. This has been identified by Davis in 1989 as Perceived Usefulness (PU). Perceived Usefulness (PU) can be interpreted as a perception of citizens of SCI to the effect that use of a technology will substantially improve performance of citizens of SCI for Prevention of Cybercrimes in SCI (PCS). It is pertinent to mention here that PU includes effectiveness, performance, trust, risk perception and productivity (Handerson, & Devett, 2003; Aggelidis, & Chatzoglou, 2009; Park, 2009; Turner, Kitchenham, Brereton, Charters, & Budgen, 2010). This variable PU is found to have appreciable impact over Actual Technology Use (ATU). Judged from the above discussions, the following hypothesis is developed.

H6: Perceived Usefulness (PU) has positive impact on Actual Technology Use (ATU).

3.7 Perceived Ease of Use (PEU): This belief has been lent from the Technology Acceptance Model (TAM) advanced by Davis, 1989 and Davis, Bagozzi and Warshaw, 1989. This factor influences the citizens to use a technology if the citizen finds that such use is not complex but easy on the contrary. This belief is construed to be a degree through which citizen believes that some efforts are needed to learn use of a technology necessary (Park, 2009). If the citizen perceives that use of that technology would not pose any constraint, the citizen would feel easy and use the technology (Handerson, & Devett, 2003). Again, this factor PUE includes ingredients like simplicity, compatibility and self-efficacy (Yi, Liau, Haung, & Hwang, 2009). This belief is considered to have impact on Actual Technology Use (ATU) since the users feel comfortable in the use of technology. With these considerations, the following hypothesis is prescribed.

H7: Perceived Ease of Use (PEU) has a positive impact on Actual Technology Use (ATU).

3.8 Entities Spreading Awareness (ESA): There are many entities which can address cybercrimes. However, studies of literature have revealed that so far as SCI is concerned, the

entities which would be able to spread awareness among citizens of SCI most effectively for prevention of cybercrimes are government initiative (GI), social media (SM) (Edelman, 2010), WoM (Hung, & Lai, 2013), organisations (Singh, H., 2015) and law enforcement (LE) (Aggarwal, 2015). Therefore, in the context of developing awareness of cybercrimes (AOC) among the citizens of SCI, it has been considered that Entities Spreading Awareness (ESA) in this context constitutes these five ingredients like GI, SM, WOM, ORG, and LE. Once the awareness of the citizens of proposed SCI towards consequences of cybercrimes increases, they would feel the need, that to prevent cybercrimes they are to use preventive technology. Then, they would be involved in Actual Technology Use (ATU) for prevention of cybercrimes (Brown, Pope, & Voges, 2003; Pevlou, & Fygenson, 2006). With these inputs, the following hypothesis is developed.

H8: Awareness of Citizens (AOC) of SCI has positive impact towards citizens' behavior to Actual Technology Use (ATU).

3.9 Awareness of Cybercrimes (AOC): AOC is associated with level of knowledge and attention which assists the users of internet (netizens) to conceptualize regarding what an internet is, how it can work and function, what are its environments, how transactions are to be done through internet safely, what are its uses and misuses, how remedies can be achieved in case of vulnerable threats, what are the laws available to address cybercrimes and so on. These ingredients will be able to assess the level of users' awareness and extent of understandabilities of cybercrimes in SCI (Avais, & Abdullah, 2014; Agarwal, 2015). Improvement of awareness among the citizens of SCI regarding cybercrimes would be an effective issue to efficiently prevent cybercrimes (Aparna, & Chauhan, 2012; Mehta, & Singh, 2013; Singeravelu, & Pillai, 2014; Parmer, & Patel, 2016). The study in the city of Anand (Gujrat, India) revealed that 68% of the netizens did not hear the term 'cyber cells' and do not know wherefrom remedies may be obtained to address cybercrimes save approaching police. 15% know about IT Act, 2000 (India); 43% know that in case of being victims of cybercrimes, IT Act, 2000 (India) is the remedy, but they never referred to that; 24% heard about IT Act 2000 of India, but do not know what this act does. 18% have hardly any idea about IT Act, 2000 of India (Narahari, & Shah, 2016). It is pertinent to mention here that in Gujrat, through Public-Private-Partnership model, a Smart City known as GIFT city (Gujrat Industrial Finance Tec-city) is in operation partially. This is the first partially operated Smart City in India. It is the first International Finance Service Center in India. That is why it is relevant to take up to assess the extent of awareness of the citizens of a city in the state of Gujrat. Judged from this important stand point, the following hypothesis is formulated.

H9: Awareness of Cybercrimes (AOC) positively affects Prevention of Cybercrimes (PCS) in SCI.

3.10 Actual Technology Use (ATU) and Prevention of Cybercrimes in SCI (PCS): The sense of Actual Technology Use (ATU) is associated with the conception that the citizens of SCI are involved with use of technology (Sorebo, Sorebo, & Sein, 2007). Once the citizens start adopting the preventive technologies and use those and once the awareness is increased, the citizens of SCI are expected to be able to prevent the cybercrimes in SCI (Longstaff, & Schultz, 1993; Abdul Nasser, 2012). With this conception, the following hypothesis is provided.

H10: Actual Technology Use (ATU) has a positive impact on Prevention of Cybercrimes in SCI (PCS).

In developing the hypotheses, we have observed that some entities like GI, SM, WOM, ORG and LE act as effective and efficient factors to prevent cybercrimes in SCI. These five factors constitute Entities Spreading Awareness (ESA). These factors impact on developing Awareness of Cybercrimes (AOC) among the citizens of India. Again, this awareness impacts significantly and positively on Prevention of Cybercrimes in SCI (PCS) (Burn, Whitworth, & Thomson, 2004; Kim, & Eastin, 2011; Hung, & Lai, 2015; Singh, 2015; Narahari, & Shah, 2016). Again, we have seen as awareness is increased, the citizens of SCI would like to be involved in Actual Technology Use (ATU) instrumental to Prevention of Cybercrimes in SCI (PCS) (Shin, 2013). Besides, the citizens of SCI would use the preventive technologies for prevention of cybercrimes in SCI only when they find the usefulness of that technology and when they would find ease to use that technology as provided in TAM, 1989 (Davis, 1989; Davis, Bagozzi, & Warshaw, 1989). All the inputs available here are shown in Table 2 as a summary.

With all these inputs including gathering knowledge from the hypotheses so developed, the following conceptual model is provided for prevention of cybercrimes in SCI and it is shown in Figure 1.

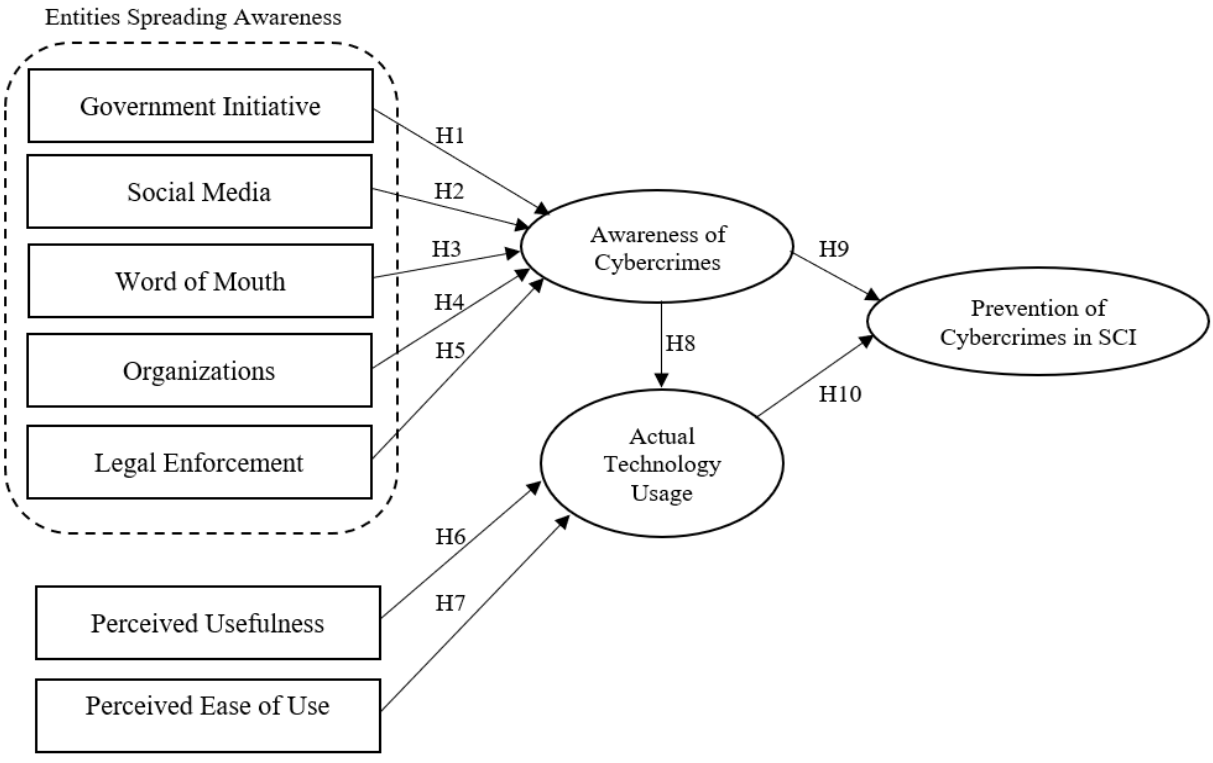


Figure 1: Conceptual Model connecting the constructs

4. Research Methodology

We have developed the constructs with the help of inputs available from literature study as well as from studies of different adoption theories including TAM (Davis, 1989). We have also analysed different research studies dealing with the different issues of adoption as well as of awareness (Ali, 2016; Narahari, & Shah, 2016; Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2017; Dwivedi, Rana, Janssen, Lal, Williams, & Clement, 2017). We have developed the conceptual model shown in figure 1. This model and the hypotheses are required to be validated with the help of standard statistical tools.

We are to frame some congenial questionnaires (items) with the help of the knowledge of constructs and with the help of existing different adoption theories and models with a special focus on TAM (Davis, 1989). After developing the initial survey instrument, we have consulted with 10 experts. They have adequate knowledge concerning to cybercrimes. They possess insights regarding development of awareness among the citizens of SCI concerning the menace of cybercrimes. Out of these 10 experts, 4 have been considered from academic areas and the remaining 6 have been considered from industries. Experts coming from academic sides are all PhD holders having knowledge of cybersecurity and smart city. The remaining 6 experts from industries have all more than 10 years' experience in R&D sections dealing mainly with cybercrime protection mechanisms. We could initially prepare 41 questions. But, as per the opinion of these 10 experts, 9 questions have been rejected. According to their opinion, out of 9 questions, some were not congenial to fetch accurate results. Some suffered from the defect of readability. Hence, we started our survey works with 32 questions covering six constructs. The questionnaires were serially oriented in such a fashion as initial questions were easy to respond. With progress, they required more deliberations. In preparing the questionnaires, we followed standard guidelines. Attention was given in structuring the questionnaires towards their layout, design, and easiness. No ambiguous question was framed. The recitals of questionnaires are shown in Appendix.

To target respondents for conducting the survey, we depended on the knowledge and information derived from the different participants attending eight different conferences and workshops in various parts of India. The theme of each conference was related to cyber security, information risk and smart cities. We targeted inhabitants of Mumbai, Gujrat, Pune, Bangalore and Delhi for conducting our survey works using convenience sampling. Here the respondents were so selected as they could be accessed conveniently. Here in this study, we have selected these five cities since these conferences were held during October 2017 to January 2018 in those places. The themes of these conferences were identical with the subject matter of this study. Thus, convenience sampling was considered appropriate. By the contacts with these participants in those workshops and conferences, we could gather list of persons inhabiting in these cities having knowledge of cybercrimes and conception of SCI.

The total prospective respondents were 483 initially. Some of the email addresses, telephone numbers or postal addresses of the prospective respondents were found inadequate and vague. They are 77 in number. So, we had to start with 406 respondents. The respondents were of different ages with different educational qualifications and professions. The 32 questionnaires were sent to 406 respondents partly through emails and partly through hardcopies. One-month

time was given for responses. We eventually received 332 responses in time. The responses were given to those 10 experts for their opinion. They opined that out of those 332 responses, 17 responses were inappropriate and opined not to consider those. Hence, we began with 315 effective and useable responses for our study. This is within acceptable limit as we know that effective responses should be more than 4 times the questionnaires and preferably should be within 10 times of the concerned questionnaires (Hinkin, 1995). Our effective responses were 315 against 32 questions. Hence, our survey approach is within permissible range. The sample demographics of these 315 responses are shown in Table 3. To quantify the responses, we used 5-point Likert Scale with marking Strongly Disagree as 1 to Strongly Agree as 5. The survey works including one-month time of responses were conducted for 4 months from October 2017 to January 2018.

5. Research Results

In the subsequent subsections, we would discuss the results obtained from the survey. At first, an overview of the demographic profile is presented, followed by the reliability analysis. This is followed by the tests for multicollinearity and validation of the model, including Structural Equation Modeling.

5.1 Respondents' Demographic Profile: The result indicates that majority of the respondents was from comparatively younger generation, for example, 59.3% of the respondents have age group from 21-40 years. In terms of occupation, it appears that 46.7% respondents were from corporate sector. As per education of the respondents, it appears that 58.4% representation came from graduate and postgraduate levels. The details are given in the Table 3.

Table 3: Demographic profile of respondents

Category		**Number**	**Percentage (%)**
Gender	Male	212	67.3
	Female	103	32.7
Age	< 20 years	26	8.2
	21-30 years	117	37.1
	31-40 years	70	22.2
	41-50 years	62	19.7
	> 50 years	40	12.8
Highest Education	SE (Secondary Education)	28	8.9
	HS (Higher Secondary)	66	20.9
	Gr (Graduate)	62	19.7
	PG (Post Graduate)	122	38.7
	Above PG (Above Post Graduate)	37	11.8
Profession	Teacher	70	22.2
	Corporate	147	46.7
	Businessman	65	20.6
	Others	33	10.5

Note: SE ≡ Secondary Education, HS ≡ Higher Secondary, Gr ≡ Graduate, PG ≡ Post Graduate, Above PG ≡ Above Post Graduate

5.2 Construct reliability test: To test the reliability of the constructs, Cronbach's alpha of each construct was computed. It has been found that the value of each Cronbach's alpha relating to each construct is more than 0.6 which is the lowest acceptable value of Cronbach's alpha. The result confirms that constructs so developed are reliable (Hair, Anderson, Tatham, & Black, 1992). The results are shown in Table 4.

Table 4: Estimation of Cronbach's alpha

Construct	Value of Cronbach's alpha	No. of Item
Entities Spreading Awareness (ESA)	0.896	17
Perceived Usefulness (PU)	0.821	3
Perceived Ease of Use (PEU)_	0.962	3
Awareness of Cybercrimes (AOC)	0.799	3
Actual Technology Use (ATU)	0.811	3
Preventing Cybercrimes in SCI (PCS)	0.867	3

5.3 Test of multicollinearity: If the constructs so developed are found close to each other in their inner meaning, it is said that identification of constructs suffers from the multicollinearity defect. It creates difficulties to apply regression analysis. For this, Variance Inflation Factor (VIF) of each construct is to be computed. It appears that each value of VIF lies between 3.3 and 5 which confirms that the constructs do not suffer from the multicollinearity defect (Kock and Lynn, 2012). The results are shown in Table 5.

Table 5: Estimation of VIF

Construct	Estimation of VIF
Entities Spreading Awareness (ESA)	3.8
Perceived Usefulness (PU)	4.2
Perceived Ease of Use (PEU)_	4.3
Awareness of Cybercrimes (AOC)	4.7
Actual Technology Use (ATU)	4.9
Prevention of Cybercrimes in SCI (PCS)	4.6

5.4 Computations of LF, AVE, CR and MSV: To assess if each questionnaire (item) can explain its own construct, we need to find out Loading Factor (LF) of each item concerning to its own construct. The lowest permissible value of LF in this context is 0.707 (Borroso, Carrion, & Roldan, 2010). To examine the reliability of each construct, we have estimated Average Variance Extracted (AVE) of each construct, Composite Reliability (CR) of each construct and Maximum Shared Variance (MSV) of each construct (Fornell, & Larcker, 1981). Acceptable lowest values of AVE and of CR are 0.5 and 0.7 respectively and each MSV should be less than its corresponding AVE (Urbach, & Ahlemann, 2010; Hair, Ringle, & Sarstedt, 2011). The entire result is shown in Table 6. The values so estimated show that they are within permissible limit. Hence, they confirm reliability of the items. It reconfirms reliability of the constructs so identified.

Table 6: Estimation of LF, AVE, CR and MSV

Construct/Item	Loadings	AVE	CR	MSV
Entities Spreading Awareness (ESA)		0.734	0.799	0.414
ESA1	0.872			
ESA2	0.866			
ESA3	0.915			
ESA4	0.844			
ESA5	0.911			
ESA6	0.867			
ESA7	0.810			
ESA8	0.812			
ESA9	0.876			
ESA10	0.895			
ESA11	0.888			
ESA12	0.871			
ESA13	0.800			
ESA14	0.842			
ESA15	0.861			
ESA16	0.799			
ESA17	0.820			
Perceived Usefulness (PU)		0.694	0.711	0.296
PU1	0.799			
PU2	0.886			
PU3	0.812			
Perceived Ease of Use (PEU)		0.709	0.792	0.361
PEU1	0.872			
PEU2	0.810			
PEU3	0.844			
Awareness of Cybercrimes (AOC)		0.735	0.801	0.365
AOC1	0.886			
AOC2	0.812			
AOC3	0.872			
Actual Technology Use (ATU)		0.715	0.742	0.348
ATU1	0.800			
ATU2	0.864			
ATU3	0.871			
Prevention of Cybercrimes in SCI (PCS)		0.753	0.796	0.365
PCS1	0.800			
PCS2	0.888			
PCS3	0.911			

It appears that values of AVE have range from 0.694 to 0.753, LFs have range from 0.799 to 0.915, CR values have range from 0.711 to 0.801. It also appears that each value of MSV is less than the corresponding value of AVE relating to each construct.

5.5 Discriminant Validity Test: If it is seen that each item concerning to its own construct is strongly associated with that construct and weakly related with other constructs, it is said that the Discriminant Validity has been established (Fornell, & Larcker, 1981). To test this, we have computed Average Variance (AV) of each construct. It is square root of the corresponding AVE. We have found that values of AV are all greater than the correlation coefficients of the construct with the other constructs. This confirms that Discriminant Validity has been established (Barclay, & Smith, 1997). The values of AV are shown in diagonal positions of the Table 7 and the values of correlation coefficients are shown in off-diagonal positions of the Table 7.

Table 7: Discriminant Validity Test

	ESA	PE	PEU	AOC	ATU	PCS	AVE
ESA	0.857						0.734
PE	0.644	0.833					0.694
PEU	0.611	0.409	0.842				0.709
AOC	0.437	0.511	0.601	0.857			0.735
ATU	0.532	0.517	0.409	0.410	0.846		0.715
PCS	0.411	0.544	0.509	0.604	0.590	0.868	0.753

There is another procedure for establishing discriminant validity test. In that case LF of each item corresponding to its own construct should be greater than the cross-loading factors of that item corresponding to other constructs. In that case, we are to find out item wise LFs and cross-loading factors. We have computed those. The entire results are shown in the Appendix. It appears that the LFs are all greater than their cross-loading factors. By this way, we have been able to reconfirm the discriminant validity test.

5.6 Structural Equation Modeling: Structural Equation Modeling (SEM) estimates the relationship prevalent among the latent variables. Computation of different parameters has been done with the application of AMOS 22. It helps to confirm whether the structure is correct and in order, whether the structure has been able to represent the data. The results are shown in Table 8.

Table 8: Model fit summary relating to the research model

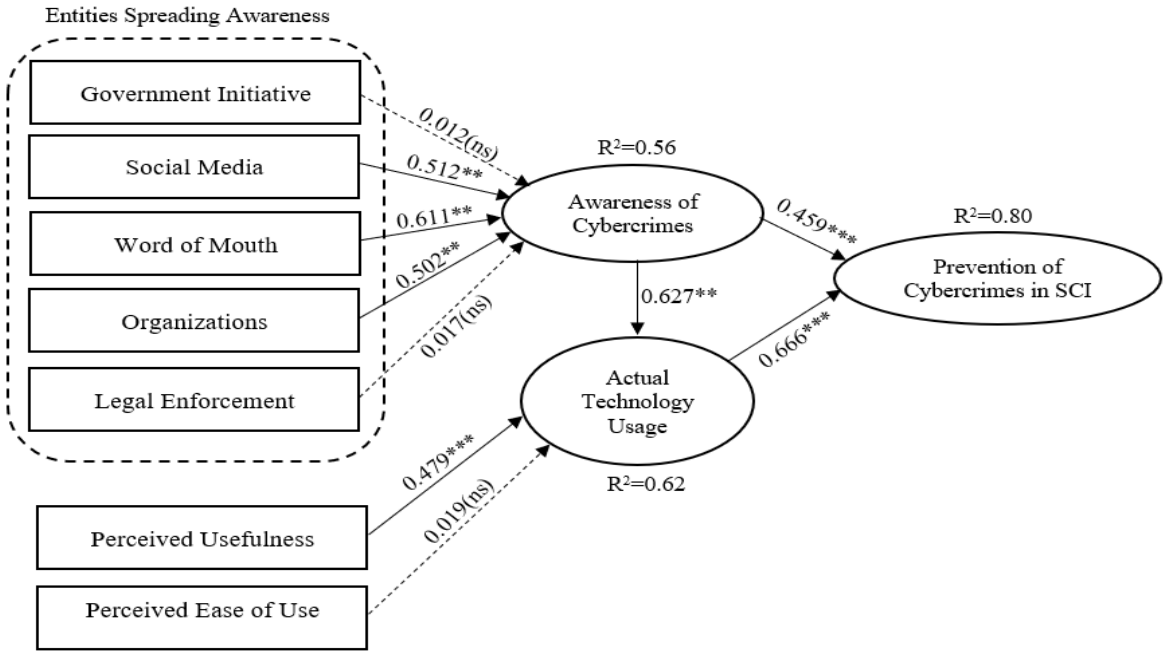
Fit Index	Recommended value	Value in the model
Chi-Square ($\chi 2$)/Degree of Freedom (df)	≤ 3.000 (Chin, & Todd, 1995; Gefen, 2000)	2.013
Goodness of Fit Index (GFI)	≥ 0.900 (Hoyle, 1995)	0.903
Adjusted Goodness of Fit Index (AGFI)	≥ 0.800 (Segars, & Grover, 1993)	0.869
Comparative Fit Index (CFI)	≥ 0.900 (Hoyle, 1995)	0.962
Tucker Lewis index (TLI)	≥ 0.950 (Hu, & Bentler, 1999)	0.957
Root Mean Square Error (RMSE)	≤ 0.080 (Hu, & Bentler, 1999)	0.026

The Table 8 shows that all fit indices are within their acceptable limits. Thus, we have been able to establish relative adequacy of the model fit. The detailed results containing paths, hypotheses, β-values, p-values are shown in the Table 9.

Table 9: Detailed results

Path	Hypothesis	Path coefficient (β-value)	p-value	Remarks
GI→AOC	H1	0.012	ns ($p > 0.05$)	Not Supported
SM→AOC	H2	0.512	** ($p < 0.01$)	Supported
WOM→AOC	H3	0.611	** ($p < 0.01$)	Supported
ORG→AOC	H4	0.502	** ($p < 0.01$)	Supported
LE→AOC	H5	0.017	ns ($p > 0.05$)	Not Supported
PU→ATU	H6	0.479	*** ($p < 0.001$)	Supported
PEU→ATU	H7	0.019	ns ($p > 0.05$)	Not Supported
AOC→ATU	H8	0.627	** ($p < 0.01$)	Supported
AOC→PCS	H9	0.459	*** ($p < 0.001$)	Supported
ATU→PCS	H10	0.666	*** ($p < 0.001$)	Supported

After validation through standard statistical tools, the model is represented in figure 2. It is the Validated Model.



ns p > 0.05; *p < 0.05; **p < 0.01; ***p < 0.001

Figure 2. Structural model with path weights and with level of significance

6. Discussions

From studies of literature, we considered that Government Initiative, effect of Legal Enforcement would influence the citizens of SCI towards improvement of their awareness of cybercrimes (Ali, 2011). We hypothesized accordingly H1 and H5. We also considered that Perceived Ease of Use would impact on Actual Technology Use (Handerson, & Devett, 2003). We hypothesized accordingly H7. But, after validation, it appears that our assumptions based on literature review have been contradicted. H1, H5 and H7 have not been supported. Studies of literature helped us to hypothesize that Social Media, Word of Mouth, Organisations have significant impacts on Awareness of Cybercrimes (Kim, & Park, 2013; Wisman, 2013; Harpreet Singh, 2015). These presumptions corresponding to H2, H3 and H4 respectively were found correct after validation. Impact of Perceived Usefulness on Actual Technology Use, impact of Awareness of Cybercrimes on Actual Technology Use, impact of Awareness of Cybercrimes on Prevention of Cybercrimes in SCI and impact of Actual Technology Use on Prevention of Cybercrimes in SCI have been considered through literature review (Davis, 1989; Sorebo, Sorebo, & Sein, 2007; Abdul Naser, 2012; Agarwal, 2015). This consideration received support from the validation results. H6, H8, H9 & H10 have been supported.

We have conceptually hypothesized 10 hypotheses and developed a model shown in figure 1. But, while we examined its validity through statistical tools, we found that out of the 10 hypotheses, 3 hypotheses were not supported. These are impact of Government Initiative (GI) on Awareness of Cybercrimes (AOC) (H1) since the path coefficient (β-value) is found to be low (0.012) having no significance level (p > 0.05). Again, impact of Legal Enforcement (LE) on Awareness of Cybercrimes (AOC) (H5) was not supported since the path coefficient (β-

value)was found low like 0.017 having no significance level ($p > 0.05$). Besides, result also shows that impact of Perceived Ease of Use (PEU) has no significant impact on Actual Technology Use (ATU) (H7), as the corresponding path coefficient (β-value) is low like 0.019 with no significance level ($p > 0.05$). Thus, out of 10 hypotheses, it is seen that 7 hypotheses have been supported like SM→AOC (H2) as its path coefficient (β-value) is as high as 0.512 with significance level $p < 0.01$. Again, WOM→AOC (H3) has been supported as its path coefficient (β-value)is 0.611 with significance level $p < 0.01$. ORG→AOC (H4) has been supported since the concerned path coefficient (β-value) is 0.502 with significance level $p < 0.01$. The PU→ATU (H6) has been supported since the path coefficient(β-value) is 0.479 having significance level $p < 0.001$. Again, AOC→ATU (H8) has been supported since the path coefficient(β-value)is 0.627 with significance level $p < 0.01$. AOC→PCS (H9) has been supported as the concerned path coefficient(β-value)is 0.459 with significance level $p < 0.001$. Again, ATU→PCS (H10) has been supported as the corresponding path coefficient (β-value) is 0.666 with significance level $p < 0.001$. Thus, hypotheses H2, H3, H4, H6, H8, H9 & H10 have been supported while hypotheses H1, H5 and H7 have not been supported. The result shows that GI, SM, WOM, ORG & LE can explain AOC to the extent of 56%, as the concerned R^2 value is 0.56. Besides, PU, PEU and AOC can explain ATU to the tune of 62% as the concerned R^2value is 0.62. Moreover, PCS can be explained by AOC and ATU to the tune of 80% as the corresponding R^2 is 0.80. Studies highlight that out of the determinants GI, SM, WOM, ORG and LE constituting the construct ESA impacting AOC, the factor WOM has strongest impact on AOC and GI has weakest impact over AOC since the corresponding path coefficients (β-values) are 0.611 and 0.012, respectively. Influence on ATU by PU is appreciable whereas impact of PEU on ATU is insignificant since the corresponding path coefficients(β-values)are 0.479 and 0.019, respectively. Influences of AOC and of ATU on PCS have been studied. It is found that out of these two constructs influencing PCS, the influence of ATU is more than the influence of AOC since the corresponding path coefficients (β-values) ATU→PCS is more (0.666) than that of AOC→PCS (0.459). The reason for such variation of influence by several factors on AOC and on ATU and on PCS will be explained in the subsequent sections.

6.1 Theoretical Implications: Our study has proposed and tested a theoretical model with AOC and ATU as two variables representing the individual context. Through analysis of our theoretical model, it appears that it has good performances since eventually it could explain 80% of the PCS. This is because that while developing the theoretical model, we selected better-suited measures instead of directly using any standard model. We had analysed the contexts exhaustively. Inclusion of AOC as a construct has added more theoretical value to the model because this construct effectively influences PCS directly.

Again, in considering the factors that would affect AOC, we did not consider many factors as it is found in the other studies. The factors like ethics, attitude, awareness was taken into consideration (Ali, 2016) to explain awareness. But in the context of improvement of AOC, we did not consider those factors in the context of our theoretical mode (Mohit, 2012). We have developed our theoretical model with consideration of five factors like GI, WOM, SM, ORG, and LE. These five factors constitute ESA. This construct ESA appreciably impacts AOC. Again, AOC in turn impacts PCS. It is our goal in this study. It has path coefficient (β-value) 0.459 with significance level $p < 0.001$(***). While considering the factors affecting ATU, we took help of TAM (Davis, 1989) and considered that PU and PEU would impact on ATU. While

considering impact on ATU, we did not consider factors like performance, effectiveness, trust, risk perception, simplicity, compatibility and self-efficacy of the technology though some researchers gave much stress on some of these factors (Lewis, & Weigert, 1995; Kim, 2005). Since PU includes performance, effectiveness, trust and risk factors (Park, 2009) and PEU includes simplicity, compatibility and self-efficacy (Yi, Liao, Huang, & Hwang, 2009), consideration of these factors separately was redundant.

This proposed theoretical model considers only some important and simple salient factors to explain PCS. Therefore, it is expected that this model will be used by the authorities and policy makers with ease. The explanatory power of this theoretical model is 80%. This high explanatory power of this theoretical model is presumably due to its simplicity and due to inclusion of AOC and of ATU as mediating variables. The theoretical proposed model has been able to explain 80% of the PCS. This indicates that non-consideration of any type of moderator influencing individuals' behavioral pattern could not adversely affect the efficiency of this proposed theoretical model. Criticism may be there for non-inclusion of the moderators in our proposed model. It may be argued that, in that case, the explanatory power might have been more than 80%. Policy makers and authorities would be able to apply this theoretical model to combat cybercrimes in SCI.

7. Conclusion

In this study, we have identified some factors that would impact on improving AOC among the citizens of SCI. Among the awareness factors constituting ESA, it appears that GI has insignificant impact on the AOC among the citizens of SCI. This lack has been criticized by the researchers. They opined that this is owing to slow working bureaucratic systems that fail to account emerging problems. This is owing to lack of preparedness to face various technologies being used by the efficient cyber criminals (Hinduja, 2004; Moitra, 2005). Besides, the LE has no significant effects on AOC among citizens of SCI. The laws which help to punish the delinquents for commission of cybercrimes are not so forceful (Mc Connel, 2000). The laws are also found not befitting and not up to date to address the cybercrimes. This is because that new nature of crimes is emerging based on updated technologies (Correia, & Bowling, 1999; Atoum, Otoom, & Ali, 2014). This is due to reluctance of police people to investigate cybercrimes with the help of existing cyber laws. They are found more agile to act against crimes of traditional nature (Goodman, 1997). LE against cybercrimes is not gaining momentum due to lack of intimate connection between investigators and prosecutors (Davis, 2012). The concerned authorities are to brush up these defects effectively.

It is recommended to update the authorities for gaining better understanding to address the rapidly evolving cybertechnologies adopted by the cyber criminals (Gogolin, & Jones, 2010). For this, attention is to be focused on updating existing laws commensurate with advancement of technologies. Efficiencies of specialized task force expected to work in SCI are to be enhanced. Effective promotion on cybercrime research activities is to be ensured. Effective utilization of civic resources available in SCI is to be made. Gathering sad experience of 9/11 attack, experts opined that cyber terrorists may attempt to damage information infrastructure and to damage key

websites of different countries (Levi, & Wall, 2004; Davis, 2012). Such untoward attack by cyber criminals may damage the very growth of SCI. It is imperative for the authorities to formulate comprehensive plan towards the best to get all the stakeholders of SCI prepared for the worst.

It is necessary to take technological, legal and organisational pragmatic approaches to make the citizens of SCI aware for prevention of cybercrimes. To detect crimes of traditional nature, identification of fingerprints and DNA helps a lot. This is not available to detect cybercriminals. For this, it is suggested that IT facilities in SCI are to be appropriately enhanced for analysing cybercrimes and for detecting cybercriminals' behavioural pattern (O. de Vel, Anderson, Carney, & Mohay, 2001). Once these are achieved, the citizens of SCI will realize that laws are being able to punish the cybercriminals effectively and quickly. Then the citizens of SCI will be influenced by the LE and their AOC will be increased. Besides, our findings show that AOC mediates the effect of ESA which constitute GI, WOM, ORG, LE, SM on ATU. This ATU impacts on PCS. AOC has a direct effect on PCS.

Besides, utilising idea of TAM, we have been able to substantiate that at least PU has a direct effect on ATU by the citizens of SCI. This, in turn, helps to prevent cybercrimes. Thus, our empirical investigation highlights that proposed theoretical model may serve as a meaningful weapon to prevent cybercrimes. When SCI will be operational, this model would act as an effective instrument to combat cybercrimes in SCI. The citizens of SCI would then unhesitatingly use ICT to meet their needs.

Finally, when the entire results are summarised, we have reached the following key findings:

- Prevention of cybercrimes in India, especially in the smart city context, is important for successfully delivering digital services in SCI.
- Entities such as WoM and SM are key contributors for spreading AOC among the citizens of SCI.
- The use of preventive technologies plays significant role for prevention of cybercrimes if the citizens can realize that the technologies are useful.
- The research studies highlight that the key determinants AOC and ATU being the mediating variables have maximum influence towards PCS.
- Finally, a theoretical model is developed for prevention of cybercrimes.

7.1 Practical and Policy Implications: The purpose of this study is to identify the factors that will be able to prevent cybercrimes. This has become necessary because in SCI, the citizens are expected to use ICT to meet their needs (Tryfons, Kiountouzis, & Poulymenakou, 2001). The government is also expected to take initiatives to involve the citizens to use ICT to make them smarter (Kickbusch, & Gleicher, 2014). This would enhance the living standard of the citizens of SCI (Foster, & Rosenzweigh, 2010). The citizens of SCI would not use technology with the help of ICT if they feel that in using ICT, they would become victims of cybercrimes (Thompson, Von Solms, & Lauw, 2006). Hence, they are to be made aware regarding the cybercrimes and its consequences. In making the citizens aware, there are various factors that would improve

awareness for prevention of cybercrimes. These factors constitute ESA. This has been included in our model.

The result of the model shows that GI has insignificant impact on AOC. For this, H1 was not supported while validating the conceptual model. The government or the policy makers need to significantly improve their initiatives to make the citizens of SCI aware regarding cybercrimes to help preventing cybercrimes. The social media has significant impact on the citizens of SCI towards improvement of their awareness regarding cybercrimes. So, the social media can be used extensively to improve awareness of the citizens of SCI for preventing cybercrimes. WoM has significant impact over AOC as is evident from the result. Thus, WoM acts as a significant ingredient that helps spreading AOC among the citizens of SCI. In smart cities, all the organisations are expected to use electronic media extensively for spreading their business activities. Thus, it is seen that organisations may also play pivotal role to enhance AOC. It is seen that LE does not affect AOC in a significant way. Thus, government and policymakers are to improve enforcement of laws to increase AOC amongst the citizens of SCI.

Improvement of AOC would enhance the use of preventive technologies by the citizens of SCI to prevent cybercrimes. Actual usage of preventive technologies by the citizens of SCI would ensure PCS as is evident from the result. It is seen from the result that the PEU has insignificant influence on the AUT, but, on the other side, PU has a positive impact towards AUT. In practice, it is evident that citizens of SCI think that technology can play pivotal role towards protecting cybercrimes in SCI. This in turn encourage citizens of SCI to use technology for prevention of cybercrimes. The citizens think that the use of technology to prevent cybercrimes is difficult to learn as is found from the result. Thus, the policy makers and the smart city authorities need to make the citizens aware and the citizens should be trained to use different smart techniques with ease to prevent cybercrimes. This would enhance the ATU by the citizens of SCI to prevent cybercrimes. However, it is expected that the authorities will be able to use the proposed theoretical model to effectively prevent cybercrimes.

7.2 Societal Implications: GoI has taken sincere initiatives to create 100 smart cities in India. For this, works are going on in full swing. When the SCI will be operational, the citizens would be involved in digital activities. The society would evolve as ‘digital society’ or ‘cyber society’. In cyber society, there will be innumerable cyber activities. This could invite influx of cybercrimes. With passage of time, the number of commission of cybercrimes is expected to be increased. Hence, there is a need of prevention of cybercrimes. The citizens of SCI are to be made aware regarding the menace of cybercrimes. Increase of awareness among the citizens of the society would help to prevent cybercrimes. This article has provided effective mechanisms for development of awareness among the prospective citizens regarding cybercrimes in terms of H1, H2, H3 and H4. This development of awareness has positive impact on prevention of cybercrimes.

Besides, the citizens of the cyber society by developing AOC would be motivated to use the preventive technologies against cybercrimes. Thus, use of preventive technologies in digital society is essential. Citizens of SCI are expected to use these preventive technologies if they feel that these preventive technologies would make them secured. Hence, societal needs in this

context are to avail such preventive technologies which are useful and can be operated with ease. In this study, this has been confirmed through H6, H8, H9 and H10.

7.3 Limitations and directions for future research: We have taken appropriate precautions while undertaking the analysis to come to the findings. However, our findings of this study are to be interpreted cautiously in the light of specific limitations. We have used the sense of adoption from TAM (Davis, 1989). But, it may be argued that we have developed the model without consideration of some citizen-specific factors. These are experience, voluntariness, age factor and gender factor. This might be available in other adoption related standard models. These are important moderators as they moderate behavioural patterns (Venkatesh, Morris, Davis, & Davis, 2003). We did not consider this because we have found no prior studies on which they depended on these moderators. These studies did not give any concrete information concerning contribution of these moderators too. Absence of consideration of these moderators is presumed to not have undermined our results completely. However, it may be construed as a limitation. The future researchers may consider the effects of these moderators.

Apart from the factors we have considered having impact on AOC in SCI, the future researchers may consider other additional factors like risk factors, trust factor and so on as is found to have been nurtured in other studies (William, Dwivedi, Lal, & Schwartz, 2009). The result of the study was arrived at by having inputs from a mixed sample of citizens. They had different professions. They had varied educational qualifications as it appears from the demographics of the people shown in the concerned table. The inputs were utilized to validate the conceptual model and the hypotheses. It is suggested that the future researchers should only pick and choose those personalities who had specific knowledge regarding ICT exclusively in handling cybercrimes in SCI. Here we have not considered such representations exclusively. It is not known if all the respondents in our survey works have adequate knowledge to handle for prevention of cybercrimes. We have considered representations of the people of some of the metropolitan cities of India where there exists or there would be smart cities. But, GoI has proposed 100 smart cities across the various parts of India. Hence, we ought to have considered representations from other cities. It would have helped to provide our results in a generic form. This gap was not filled up. This is left for the future researchers to nurture. Finally, in our study, we could explain the ultimate construct PCS to the tune of 80% (R^2=0.80). It is left for the future researchers to identify and test other boundary conditions in addition to provide a more comprehensive and richer realization.

References

Abu-Musa, A.A. (2008), “Information technology and its implications for internal auditing”, *Managerial Auditing Journal*, Vol. 23 No. 5, pp. 436-466.

Adams, J.M. (1996), "Controlling cyberspace: applying the computer fraud and abuse act to the internet", *Santa Clara Computer and High-Technology Law Journal*, Vol. 12, pp. 403–434.

Agarwal, G. (2015),“General Awareness on Cyber Crime”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 5 No. 8, pp. 204-206.

Aggelidis, V. & Chatzoglou, P. (2009), “Using a modified technology acceptance model in hospitals”, International journal of medical informatics, Vol. 7 No. 8, pp. 115–126.

Alalwan, A. A., Rana, N. P., Dwivedi, Y. K., & Algharabat, R. S. (2017),"Social Media in Marketing: A review and analysis of the existing literature", *Telematics and Informatics*, Vol. 34 No. 7, pp. 1177–1190.

Ali, M.M. (2016), "Determinants of Preventing Cyber Crime: A Survey Research", *International Journal of Management Science and Business Administration*, Vol. 2 No. 7, pp. 16-24.

Alomari, M., Woods, P., & Sandhu, K. (2012), "Predictors for e-government adoption in Jordan: Deployment of an empirical evaluation based on a citizen-centric approach", *Information Technology & People*, Vol. 25 No.2, pp. 207-234.

Alryalat, M., Rana, N. P., Sahu, G. P., Dwivedi, Y. K., & Tajvidi, M. (2017), "Use of social Media in Citizen-Centric Electronic Government Services: A literature analysis", *International Journal of Electronic Government Research*, Vol. 13 No. 3, pp. 55–79.

Aparna & Chauhan, M. (2012), "Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity", *International Journal of Enterprise Computing and Business Systems*, Vol. 2, No. 1, pp. 1-10.

Atoum, I., Otoom, A., & Ali, A.A. (2014), "A holistic cyber security implementation framework", *Information Technology & People*, Vol. 22 No. 3, pp. 251-264.

Avais, M.A., Wassan, A.A., Narejo, H., & Khan, J.A. (2014), "Awareness regarding cyber victimization among students of University of Sindh, Jamsharo", *International Journal of Asian Social Science*, Vol. 4 No. 5, pp. 632-641.

Bakry, S.H. (2004), "Development of e-government, A STOPE View", *International Journal of Network Management*, Vol. 14 No.5, pp. 339-350.

Barclay, D.W., & Smith, J. B. (1997). "The effects of organizational differences and trust on the effectiveness of selling partner relationships", *Journal of Marketing*, Vol. 61 No. 1, pp. 3–21.

Borroso, C., Carrion, G. C., & Roldan, J. L. (2010), "Applying Maximum Likelihood and PLS on Different Sample Sizes: Studies on Seroquel Model and Employee Behavior Model". In V. Esposito Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds.), *Handbook of Partial Least Squares: Concepts, Methods and Applications.* Heidelberg, Springer pp. 427-447.

Bowen, M. (2009), "Computer Crime". Available at: http://www.guru.net/. (accessed January 26, 2018).

Brenner, S. W., & Goodman, M. D. (2002),"The Emerging Consensus on Criminal Conduct in Cyberspace", Vol. 10 No.2, pp 139-223.

Brown, M., Pope, N. & Voges, K. (2003), "Buying or browsing? An exploration of shopping orientations and online purchase intention", *European Journal of Marketing*, Vol. 37, No. (11/ 12), pp. 1666–1684.

Burns, R., Whitworth, K. and Thompson, C. (2004), "Assessing law enforcement preparedness to address internet fraud", *Journal of Criminal Justice*, Vol. 32, pp. 477-93.

Caragliu, A., Del Bo, C., &Nijkamp, P. (2011), "Smart cities in Europe", *Journal of Urban Technology*, Vol. 16 No. 2, pp. 65-82.

Castiglione, A., Colace, F., Moscato, V. & Palmieri, F. (2018), "Technological innovations in Digital transformation", *Future Generation Computer Systems*, Vol. 86, pp. 1134-1145.

Carlino, G.A. (2011). Three keys of the city: resources, agglomeration economies, and sorting, *Business Review Quarterly*, Vol. 3, pp.1-13.

Chan, P.K, Fan, W, Prodromidis, A.L, & Stolfo, S.J. (1999), "Distributed data mining in credit card fraud detection", IEEE Intelligent System, Vol. 14 No. 6, pp. 67– 74.

Chatterjee, S., & Kar, A.K. (2017), "Successful adoption of IT enabled services in proposed Smart City of India: A critical analysis for user experience perspective", *Journal of Science and Technology Policy Management*, Available at https://doi.org/10.1108/ JSTPM-03-2017-0008.

Chatterjee, S., Kar, A.K., & Gupta, M.P. (2018), "Success of IoT in Smart Cities of India: An empirical analysis", *Government Information Quarterly*. https://doi.org/10.1016/j.giq. 2018.05.002.

Chatterjee, S., Kar, A.K., & Gupta, M.P. (2017), "Alignment of IT authority and citizens of proposed smart cities in India: System security and privacy perspective", *Global Journal of Flexible Systems Management*, Vol. 19 No. 1, pp. 95-107.

Chatterjee, S., Kar, A.K., & Gupta, M.P. (2017), "Critical Success Factors to Establish 5G Network in Smart Cities: Inputs for Security and Privacy", *Journal of Global Information Management*, Vol. 25 No. 2, pp. 15-37.

Chatterjee, S., & Kar, A.K (2015). Smart Cities in developing economies: A literature review and policy insights, International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2335-2340.

Chaturvedi, M., Singh, A.N., Gupta, M.P., & Bhattacharya, J. (2014), "Analyses of issues of information security in Indian context", *Information Technology & People*, Vol. 8 No.3, pp. 374-397.

Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J. (2003), "COPLINK: managing law enforcement data knowledge", *Communications of the ACM*, Vol. 46 No. 1, pp. 28–34.

Cheung, C. M.& Lee, M.K. (2012), "What Drives Consumers to Spread Electronic Word of Mouth in Online Consumer-Opinion Platforms", *Decision Support Systems*, Vol. 53 No. 1, pp. 218–225.

Chhonker, M.S., Verma, D. & Kar, A.K. (2017). "Review of Technology Adoption frameworks in Mobile Commerce", *Information Technology and Quantitative Management*, Vol. 122, pp. 888-895.

Chin, W. W., & Todd, P. A. (1995), "On the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution", *MIS Quarterly*, Vol.19 No. 2, pp. 237–246.

Cho, I., H. Park, & Kim, J.K. (2014), "The Relationship Between Motivation and Information Sharing about Products and Services on Facebook", *Behaviour & Information Technology*, Vol. 30 No. 1, pp. 1–11.

Chu, S. C., & Kim, Y. (2011), "Determinants of Consumer Engagement in Electronic Word-of-Mouth (e WOM) in Social Networking Sites", *International Journal of Advertising*, Vol. 30 no. 1, pp. 47–75.

Comin, D.A. &Hobijn, B. (2010), "An exploration of technology diffusion", *American Economic Review*, pp. 2031-2061. Available at https://www.dartmouth.edu/~dcomin /files/ exploration_technology.pdf (accessed on March 16, 2018).

Correia, M. and Bowling, C. (1999), "Veering toward digital disorder: computer-related crime and law enforcement preparedness", *Police Quarterly*, Vol. 2 No. 2, pp. 225-44.

Davis, F., Bagozzi, R., &Warshaw, P. (1989), "User acceptance of computer technology: a comparison of two theoretical models", *Management Science*. Vol. 35 No. 8, pp. 982–1003.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol.13 No. 3, pp. 319-340.

Davis, J.T. (2012), "Examining perceptions of local law enforcement in the fight against crimes with a cyber component", *Policing: An International Journal of Police Strategies & Management*, Vol. 35 No. 2, pp. 272 – 284.

Devaraj, S., Fan, M.& Kohli, R.(2002), "Antecedents of B2C Channel Satisfaction and Preference: Validating e- Commerce Metrics", *Information Systems Research*, Vol. 13 No. 3, pp. 316–333.

De Vel, O., Anderson, A., Corney, M., &Mohay, G. (2001), "Mining e-mail content for author identification forensics", *SIGMOD Record*, Vol. 30 No. 4, pp. 55– 64.

Dwivedi YK, Rana NP, Janssen M, Lal B, Williams MD & Clement RM. (2017), "An Empirical Validation of a Unified Model of Electronic Government Adoption (UMEGA)", *Government Information Quarterly*, Vol. 34 No. 2, pp. 211-230.

Dwivedi YK, Rana NP, Jeyaraj A, Clement M & Williams M.D. (2017), "Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model", *Information Systems Frontiers*, pp. 1-16. https://doi.org/10.1007/ s10796-017-9774-y.

Ellison, N. B. (2007), "Social Network Sites: Definition, History, and Scholarship",*Journal of Computer-Mediated Communication*, Vol. 13 No. 1, pp. 210–230.

Falconer, G., & Mitcheli. (2012),"Smart City framework: A systematic process for enabling Smart Connected Communities". Available at: http://www.cisco.com/c/dam/ en_us/about/ac79/ docs/ps/motm/Smart-City-Framework.pdf. (accessed on February 17, 2018).

Fishbein, M., & Ajzen, I. (1975),"Belief, attitude, intention and behavior: An introduction to theory and research", Reading, MA: Addison-Wesley.

Fornell, C., & Larcker, D. F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, vol. 18 No. 1, pp. 39–50.

Foster, A.D. and Rosenzweig, M.R. (2010), "Microeconomics of technology adoption", *Economic Growth Center, Yale University*, discussion paper No. 984.

Gatzlaff, K.M. and Mccullough, K.A. (2010), "The effect of data breaches on shareholder wealth", *Risk Management and Insurance Review*, Vol. 13 No. 1, pp. 61-83.

Gcaza, N., Solms, R., Grobler, M.M., Vuuren, J.J.(2017), "A general morphological analysis: delineating a cyber-security culture", *Information Technology & People*, Vol. 25 No. 3, pp. 259-278.

Gefen, D. (2000),"E-commerce: The role of familiarity and trust",*The International Journal of Management Science*, Vol. 28 No. 6, pp. 725–737.

Gogolin, G. and Jones, J. (2010), "Law enforcement's ability to deal with digital crime and the implications for business", *Information Security Journal: A Global Perspective*, Vol. 19, pp. 109-17.

Gosgerove, V. (2011),"Smart Cities: Introducing the IBM city operations and management solutions", IBM.

Gros, J. (2003), "Trouble in paradise: crime and collapsed states in the age of globalization", *British Journal of Criminology*, Vol. 43, pp. 63-80.

Gul, M.S., Patidar, S. (2015), "Understanding the energy consumption and occupancy of a multipurpose academic building", *Energy and Building*, Vol. 87, pp. 155-165.

Gupta, B. B., Joshi, R.C., Misra, M. (2012), "ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack", *International Journal of Network Security,* Vol. 14, No. 1, pp. 36-45.

Gupta, R. (2014), "The Pattern of Urban Land Use Changes, A case study of Indian Cities", *Environment and Urbanization Asia*, Vol. 5 No. 1, pp. 83-104.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1992), "Multivariate data analysis with readings", (3rd ed.). New York, NY: Macmillan Publishing Company.

Hair, J. F., Ringle, C.M. & Sarstedt, M. (2011), "PLS-SEM: Indeed, a Silver Bullet", Journal *of Marketing Theory and Practice,* Vol. 19 No. 2, pp.139–152.

Harpreet Singh. (2013), "Cybercrime- a threat to persons, property, government and societies", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3 No.5, pp. 997-1002.

Henderson, R., &Divett, M. (2003), "Perceived usefulness, ease of use and electronic supermarket use", *International Journal of Human-Computer Studies,* Vol. 59 No. 3, pp. 383-395.

Hinduja, S. (2004), "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", *Policing: An International Journal of Police Strategies & Management,* Vol. 27 No. 3, pp. 341-57.

Hinkin, T.R. (1995), "A Review of Scale Development Practices in the Study of Organizations", *Journal of Management*, Vo. 21 No. 5, pp. 967-988.

Holsapple, C.W., & Lee-Post, A. (2006),"Defining, assessing, and promoting clearing success: An information systems perspective", *Journal of Innovative Education*, Vol. 4 No. 1, pp. 67-85.

Hoyle, R. H. (1995), "The structural equation modeling approach: Basic concepts and fundamental issues", Thousand Oaks, CA: Sage Publications.

Hu, L. -T., & Bentler, P. M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", *Structural Equation Modeling*, Vol. 6 No. 1, pp. 1–55.

Hung, Y. H. and H. Y. Lai. (2015), "Effects of Facebook Like and Conflicting Aggregate Rating and Customer Comment on Purchase Intentions", *International Conference on Universal Access in Human-Computer Interaction,* 193–200. Los Angeles, CA: Springer International. *Information Dimensions, Communications of the Association for Information Systems*, Vol31 No.5, pp. 1–23.

Jankowitz, H.T. (1988), "Detecting plagiarism in student PASCAL programs", *Computer Journal*, Vol. 31 No. 1.

Jiow, H. J. (2013), "Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint", *International Journal of Cyber Criminology*, Vol 7 No.1, pp 18-27.

Joshi, S.M. (2016), "Full guide on Cyber Crimes in India", *Journal of Frauds*, India Forensic Consultancy Services. http://indiaforensic.com/ (accessed on January 22, 2018).

Kaplan, A. M., & Haenlein, M. (2010), "Users of the world, unite! The challenges and opportunities of social media", *Business Horizons,* Vol. 53, No. 1, pp. 59–68.

Kelly, B.J. (1999), "Preserve, Protect and Defend", *Journal of Business Strategy,* Vol.20 No.5, pp. 22-26.

Kickbusch, I &Gleicher D. (2014), "Smart governance for health and well-being: the evidence", *Copenhagen: World Health Organization Regional Office for Europe*, pp. 106-27,

Available at http://www.euro.who.int/data/assets/pdf_file/0005/257513/Smart-governance-for-health-and-well-being-the-evidence.pdf (accessed on December 16, 2017).
Kim, S., & Eastin, M.S. (2011),"Hedonic Tendencies and the Online Consumer: An Investigation of the Online Shopping Process", *Journal of Internet Commerce*, Vol. 10 No. 1, pp. 68–90.
Kim, S.E. (2005), "The role of trust in the modern administrative state: An integrated model", *Administration and Society*, Vol 37 No.5, pp. 611-635.
Kim, S., & Park, H. (2013), "Effects of Various Characteristics of Social Commerce (s-Commerce) on Consumers' Trust and Trust Performance", *International Journal of Information Management*, Vol.33 No. 2, pp. 318–332.
Kim, Y., & Srivastava, J. (2007), Impact of Social Influence in e-Commerce Decision Making. Proceedings of the Ninth International Conference on Electronic Commerce. Minneapolis, MN, pp. 293–302.
King, R. A., Racherla, P., & Bush, V. D. (2014), "What we know and don't know about online word-of-mouth: A review and synthesis of the literature", *Journal of Interactive Marketing*, Vol. 28 No. 3, pp. 167-183.
Kock, N. & Lynn, G. (2012), "Lateral Collinearity and Misleading Results in Variance-Based SEM: An Illustration and Recommendations", *Journal of the Association for Information Systems*, Vol. 13 No. 7, pp. 546-580.
Levi, M., & Wall, D. (2004), "Technologies, Security and Privacy in the post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, pp. 194-230.
Lewis, J.D., & Weigert, A. (1985), "Trust as a social reality", *Social forces*, Vol. 63 No. 4, pp. 967-985.
Longstaff, T., Schultz, E. (1993), "Beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code", *Computers & Security*, Vol. 12, pp. 61– 77.
Lu, B., W. Fan, & Zhou, M. (2016),"Social Presence, Trust, and Social Commerce Purchase Intention: An Empirical Research", *Computers in Human Behavior*, Vol. 56, No. pp. 225–237.
Mansoori, K.A., Sarabdeen, J., & Tchantchane, A.L. (2018), "Investigating Emirati citizens' adoption of e-government services in Abu Dhabi using modified UTAUT model", *Information Technology & People*, Vol. 31 No. 2, pp. 455-481.
McConnell. (2000), "Cyber Crime and Punishment". McConnell International LLC.
Mehta, S. & Singh,V. (2013), "A Study of Awareness About Cyberlaws in the Indian Society", *International Journal of Computing and Business Research*, Vol.4, No. 1, pp. 1-8.
Michael, B., Steingruebl, A., & Smith, B.(2011), "Combating Cybercrime Principles, Policies and Program". *Paypal*. https://www.paypal-media.com/assets/pdf/fact_sheet/ PayPal_Com batingCybercrime_WP_0411_v4.pdf. (accessed on March 17, 2018).
Mikalef, P., I. O. Pappas, & M. Giannakos. (2016),"Consumer Intentions on Social Media: A fsQC Analysis of Motivations", *Conference on e-Business, e-Services and e- Society*, Swansea, Wales, UK, 371–386.
Mitnick, K.D. and Simon, W.L. (2011), "The Art of Deception: Controlling the Human Element of Security", Wiley, New York, NY.
Mohamed, C. (2003), A critical look at a regulation of cybercrime - A Comparative Analysis with Suggestions for Legal Policy. Available at: www.crime-research.org/library/Critical.doc (accessed on February 16, 2018).

Mohit, G. (2012), “Ethics and Cybercrime in India”, *International Journal of Engineering and Management Research*, Vol. 2 No.1, pp. 1-3.

Moitra, S. (2005), “Developing policies for cybercrime”, *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13 No. 3, pp. 435-64.

Muniandy, L. & Muniandy, B. (2012), “State of cyber security and the factors governing its protection in Malaysia”, *International Journal of Applied Science and Technology*, Vol. 2 No. 4, pp. 106-113.

Narahari, A.C., & Shah, V. (2016), “Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand”, *International Journal of Advance Research and Innovative Ideas in Education*, Vol. 2 No. 6, pp. 1164-1172.

National Cyber Security Policy (2013), Available at: http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf (accessed on March 12, 2018).

Obuh, A. O., & Babatope, I. S. (2011), “Cybercrime Regulation: The Nigerian Situation”. pp.7-8.

Parise, S. and Guinan, P.J. (2008), “Marketing Using Web 2.0.” In Proceedings of the 41st *Hawaii International Conference on System Sciences*, edited by R. Sprague, 281, Hawaii, HI, January 2008. Washington, DC: IEEE Computer Society Press.

Park, S. (2009), “An Analysis of the Technology Acceptance Model in Understanding University Students' Behavioral Intention to Use e-Learning”, *Educational Technology & Society*, Vol. 12 No. 3, pp. 150–162.

Parmar, Aniruddhsinh & Patel Kuntal (2016), Critical Study and Analysis of Cyber Law Awareness Among Netizens. Conference: International Conference on ICT for Sustainable Development, Available at http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Vol. 409. (accessed March 12, 2018).

Parthasarathi Pati. (2003), “Cyber-crime”, The Indian Law Institute. Available at: http://naavi.org/pati/ (accessed January 4, 2018).

Pavlou, P. A. & Fygenson, M. (2006), “Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior”, *MIS Quarterly*, Vol. 30 No. 1, pp. 115–143.

Philippsohn, S. (2001), "Trends in cybercrime—an overview of current financial crimes on the internet", *Computers & Security*, Vo. 20 No. 1, pp. 53–69.

Power, R. (2002), "CSI/FBI computer crime and security survey", *Computer Security Issues & Trends*, Vol. 8 No. 1, pp. 1 –22.

Qualman, E. (2012), “Socialnomics: How Social Media Transforms the Way We Live and Do Business”, New York, NY, John Wiley & Sons.

Raghav, S.S. (2012), “Cyber Security in India’s Counter Terrorism Strategy”. http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf (accessed on December 10, 2017).

Rana NP, Dwivedi YK, Williams MD & Weerakkody V. (2016), “Adoption of online public grievance redressal system in India: Toward developing a unified view”, *Computers in Human Behavior*, Vol. 59, pp. 265-282.

Richards, J.R. (1999), “Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers”, *Auditors, and Financial Investigators*, CRC Press, Boca Raton, FL.

Saini, H., Rao, Y.S., & Panda, T.C. (2012), "Cyber-Crimes and their Impacts: A Review", *International Journal of Engineering Research and Applications*, Vol. 2 No. 2, pp. 202-209.

Segars, A. H., & Grover, V. (1993), "Re-examining perceived ease of use and usefulness: A confirmatory factor analysis", *MIS Quarterly*, Vol. 17 No. 4, pp. 517–525.

Shaheen Dhada and Renu Shrinivas case of Maharastra (2012). http://archive.indianexpress.com /news/two-girls-arrested-for-facebook-post-questioning-bal-thackery-shutdown-ofmumbai-get-bail/1033177

Shareef, M.A, Kumar, U, Kumar, V & Dwivedi, Y.K. (2011), "E-government Adoption Model (GAM): Differing Service Maturity Levels", *Government Information Quarterly*, Vol. 28 No. 1, pp. 17-35.

Shin, D. H. (2013), "User Experience in Social Commerce: In Friends We Trust", *Behavior & Information Technology*, Vol. 32 No.1, pp. 52–67.

Shreya Singhal v. Union of India, WP (Criminal) No. 167 of 2012, Supreme Court of India.

Singaravelu, S & Pillai, K. P. (2014), "Students Awareness on Cybercrime in Perambalur District", *International Journal of Teacher Educational Research*, Vol.3 No.3.

Sorebo, A., Sorebo, O., & Sein, M. (2007), "The Influence of User Involvement and Personal Innovativeness on User Behavior", *World Academy of Science, Engineering and Technology*, Vol. 32, pp. 98-103.

Spafford, E. (1989), "The internet worm program: an analysis", *Computer Communication Review*, Vol. 19 No. 1, pp. 17–49.

Sproles, J., & Byars, W. (1998), "Cyber-terrorism". Computer Ethics at ETSU.

Sunit, B. &Nina, G. (2011), "Cyber Security: Understanding Cybercrimes, computer forensics and Legal Perspectives", First Edition, Wiley India.

Supriya, K. (2012),"Cyber Crime", *National University of Study and Research in Law*, Ranchi University, p.7.

Tagliabue, L.C., Buzzetti, M., Arosio, B. (2012), "Energy saving through the Sun: Analysis of visual comfort and energy consumption in office space", *Energy Procedia*, Vol. 30, pp. 693-703.

Thomas, D, Loader, B.D. (2000), "Introduction—cybercrime: law enforcement, security and surveillance in the information age, Cybercrime: Law Enforcement, Security and Surveillance in the Information Age", Taylor & Francis Group, New York, NY, 2000.

Thomson, K.L., Von Solms, R., & Lauw, L. (2006), "Cultivating an organizational information security culture", *Computer Fraud and Security*, Vol. 6 No. 10, pp. 7-11.

Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001), "Embedding security practices in contemporary information systems development approaches", *Information Management and Computer Security*, Vol. 9 No. 4, pp. 183-197.

Turner, M., Kitchenham, B., Brereton, P., Charters, & S., Budgen, D. (2010), "Does the technology acceptance model predict actual use? A systematic literature review", *Information and Software Technology*, Vol. 52, pp. 463–479.

Urbach, N., & Ahlemann, F. (2010), "Structural Equation Modeling in Information System Research Using Partial Least Squares", *Journal of Information Technology Theory and Application*, Vol. 11 No. 2, pp. 5-40.

Van den Bergh, J., and Viaene, S. (2015). Key challenges for the Smart City. Turning ambition into reality, *In 48th Hawaii International Conference on System Science (HICSS), Kanai, Hawaii, IEEE*, pp. 2385-2394.

Venkatesh, V., Morris, M.G., Davis, G.B. & Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-478.

Weerakkody, V., Irani, Z., Kapoor, K., Sivarajah, U., & Dwivedi, Y. K. (2017),"Open data and its usability: An empirical view from the Citizen's perspective", *Information Systems Frontiers*, Vol. 19 No. 2, pp. 285–300.

Williams, M. D., Dwivedi, Y. K., Lal, B., & Schwarz, A. (2009),"Contemporary trends and issues in IT adoption and diffusion research", *Journal of Information Technology*, Vol. 24 No. 1, pp.1–10.

Wisman, T.H.A. (2013),"Purpose and function creep by design: Transforming the face of surveillance through the IoT", *European Journal of Technology*, Vol. 4 No. 2. Available at: http://ejlt.org/article/view/192/379 (accessed January 11, 2018).

Wolfinbarger, M. & Gilly, M.C. (2001), "Shopping Online for Freedom, Control, and Fun", *California Management Review*, Vol. 43 No. 2, pp. 34–55.

Om pal, Pandey, T., Alam, B. (2017), "How to report Cybercrimes in Indian territory", *International Journal of Science, Technology and Management*, Vol.6 No. 4, pp. 166-180.

Yadav, M. S., K. De Valck, T. Hennig-Thurau, D. L. Hoffman, & Spann, M. (2013), "Social Commerce: A Contingency Framework for Assessing Marketing Potential", *Journal of Interactive Marketing*, Vol. 27 No. 4, pp. 311–323.

Yi, C., Liao, P., Huang, C., & Hwang, I. (2009), "Acceptance of Mobile Learning: a Re specification and Validation of Information System Success", *World Academy of Science, Engineering and Technology*, Vol. 53, pp.726-730.

Zaied, A.N.H. (2012),"An Integrated Success Model for Evaluating Information System in Public Sectors", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 3 No. 6, pp. 814-825.

Zhang, K. Z., & M. Benyoucef. (2016),"Consumer Behavior in Social Commerce: A Literature Review", *Decision Support Systems*, Vol. 86, pp. 95-108.

Zhao, F., Scavarda, A.J., & Waxin, M.F. (2012), "Key issues and challenges in e-government development: An integrative case study of the number one e City in the Arab world", *Information Technology & People*, Vol. 25 No. 4, pp. 395-422.

Zheng, X., Zhu, S. and Lin, Z.(2013), "Capturing the Essence of Word-of-Mouth for Social Commerce: Assessing the Quality of Online E-Commerce Reviews by a Semi-Supervised Approach", *Decision Support Systems*, Vol. 56, pp. 211–222.

Zuiderwijk, A., Janssen, M.& Dwivedi, Y.K. (2015),"Acceptance and Use Predictors of Open Data Technologies: Drawing upon the Unified Theory of Acceptance and Use of Technology", *Government Information Quarterly*, Vol. 32 No. 4, pp. 429-440.

Appendix

Table A1. Items and questionnaire

Item/Construct	Statement
Entities Spreading	

Awareness (ESA)	
ESA1	Spreading awareness on cyberthreats is important to prevent cybercrimes
ESA2	Various entities should be involved for spreading awareness on cybercrimes
ESA3	I get information on cyberthreats from different government initiatives
ESA4	Government initiatives are effective to make citizens aware of cyberattacks
ESA5	Government is doing an excellent job by spreading awareness on cybercrimes
ESA6	I use social media extensively for gathering information
ESA8	Social media provides vital information on different cyberthreats
ESA9	Social media is an important instrument combating cybercrime
ESA10	I know how to use internet securely
ESA11	All the inhabitants of smart cities of India would use social media extensively
ESA12	I learn on cyberthreats from other people
ESA13	My friends and relatives discuss about menace of cyberattacks with me
ESA14	I am aware of IT Act in India and its provisions
ESA15	Legal enforcement is essential to spread awareness on cyberthreats among citizens
ESA16	Organisations in the smart cities would play important roles on cyber awareness
ESA17	My organisation makes me aware about different cyberthreats
Perceived Usefulness (PU)	
PU1	Proper application of technology can help to prevent cybercrimes
PU2	I use different techniques to protect myself from different cybercrimes
PU3	Citizens of smart cities would use technology extensively to prevent cybercrimes
Perceived Ease of Use (PEU)	
PEU1	I find it easy to use different tools and technologies for protection of cyberthreats
PEU2	I expect most of the citizens of smart cities would find it easier to use different tools and technologies to protect themselves from cybercrimes
PEU3	I perceived that in future the technology to protect from cybercrimes would become easier to use by the citizens
Awareness of Cybercrimes (AOC)	
AOC1	I am aware of various kinds of cyberthreats
AOC2	It is important for me to know about different cybercrimes
AOC3	All the citizens in smart cities should be aware of different cybercrimes
Actual Technology Use (ATU)	
ATU1	Citizens of the smart cities should be trained how to use technology efficiently to prevent cybercrimes
ATU2	I have proper training to use different tools and technologies for protecting myself from various kinds of cybercrimes
ATU3	All the citizens in smart cities need to use different technologies extensively for preventing cybercrimes
Preventing Cybercrimes in SCI (PCS)	
PCS1	Cybercrimes can be prevented by making citizens aware
PCS2	Technology plays a vital role for preventing cybercrimes in smart cities of India
PCS3	I believe authorities would take sufficient measures for preventing cybercrimes in smart cities of India.

Table A2: Computations of loadings and cross-loadings

	ESA	PU	PEU	AOC	ATU	PCS
ESA1	**0.872**	0.432	0.462	0.491	0.417	0.451
ESA2	**0.866**	0.401	0.496	0.500	0.416	0.462
ESA3	**0.915**	0.506	0.417	0.417	0.411	0.426
ESA4	**0.844**	0.413	0.431	0.419	0.490	0.417

ESA5	**0.911**	0.333	0.437	0.418	0.491	0.471
ESA6	**0.867**	0.412	0.421	0.417	0.498	0.433
ESA7	**0.810**	0.451	0.496	0.416	0.496	0.344
ESA8	**0.812**	0.424	0.311	0.412	0.499	0.390
ESA9	**0.876**	0.416	0.392	0.492	0.501	0.311
ESA10	**0.895**	0.392	0.491	0.399	0.490	0.317
ESA11	**0.888**	0.501	0.371	0.463	0.493	0.361
ESA12	**0.871**	0.362	0.401	0.461	0.492	0.409
ESA13	**0.800**	0.492	0.388	0.490	0.490	0.416
ESA14	**0.842**	0.302	0.492	0.417	0.493	0.437
ESA15	**0.861**	0.399	0.498	0.416	0.420	0.433
ESA16	**0.799**	0.471	0.500	0.311	0.491	0.462
ESA17	**0.820**	0.490	0.490	0.408	0.496	0.411
PU1	0.417	**0.799**	0.401	0.405	0.499	0.426
PU2	0.416	**0.886**	0.392	0.393	0.491	0.431
PU3	0.438	**0.812**	0.309	0.390	0.501	0.437
PEU1	0.496	0.411	**0.872**	0.411	0.502	0.490
PEU2	0.501	0.417	**0.810**	0.416	0.490	0.411
PEU3	0.309	0.424	**0.844**	0.417	0.496	0.431
AOC1	0.412	0.416	0.419	**0.886**	0.411	0.437
AOC2	0.424	0.419	0.418	**0.812**	0.407	0.431
AOC3	0.504	0.492	0.496	**0.872**	0.431	0.492
ATU1	0.302	0.311	0.491	0.411	**0.800**	0.390
ATU2	0.409	0.317	0.317	0.417	**0.864**	0.361
ATU3	0.399	0.492	0.333	0.438	**0.871**	0.317
PCS1	0.421	0.407	0.433	0.496	0.416	**0.800**
PCS2	0.457	0.398	0.411	0.416	0.401	**0.888**
PCS3	0.450	0.390	0.407	0.490	0.419	**0.911**

Table A3: Statement of hypothesis and remarks

Hypothesis	**Statement**	**Remarks**
H1	Government Initiatives (GI) would positively impact on Awareness of Cybercrimes (AOC).	Not Supported

H2	Social Media (SM) will have positive impact to enhance Awareness of Citizens (AOC) of SCI towards cybercrimes.	Supported
H3	Word of Mouth (WOM) has a positive impact over Awareness of Cybercrimes (AOC) among the citizens of SCI.	Supported
H4	Organisations (ORG) have positive impact on the Awareness of Cybercrimes (AOC) among the citizens of SCI.	Supported
H5	Legal Enforcement (LE) has a positive impact on the Awareness of Cybercrimes (AOC) of the citizens of SCI.	Not Supported
H6	Perceived Usefulness (PU) has positive impact on Actual Technology Use (ATU).	Supported
H7	Perceived Ease of Use (PEU) has a positive impact on Actual Technology Use (ATU).	Not Supported
H8	Awareness of Citizens (AOC) of SCI has positive impact towards citizens' behavior to Actual Technology Use (ATU).	Supported
H9	Awareness of Cybercrimes (AOC) positively affects Prevention of Cybercrimes (PCS) in SCI.	Supported
H10	Actual Technology Use (ATU) has a positive impact on Prevention of Cybercrimes in SCI (PCS).	Supported

Table A4: Path Analysis

	β-value	**Hypothesis**	**p-value**	**R^2**	**Remark**
Effect on AOC				0.56	
by GI	0.012	H1	ns ($p > 0.05$)		Not supported
by SM	0.512	H2	** ($p < 0.01$)		Supported
by WOM	0.611	H3	** ($p < 0.01$)		Supported
by ORG	0.502	H4	** ($p < 0.01$)		Supported
by LE	0.017	H5	ns ($p > 0.05$)		Not supported
Effect on ATU				0.62	
by AOC	0.627	H8	** ($p < 0.01$)		Supported
by PU	0.479	H6	***($p < 0.001$)		Supported
by PEU	0.019	H7	ns ($p > 0.05$)		Not supported
Effect on PCS				0.80	
by AOC	0.459	H9	***($p < 0.001$)		Supported
by ATU	0.666	H10	***($p < 0.001$)		Supported