Volume 6, Issue 1, January 2019 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

# Investigating Citizen's Awareness of Privacy and Security Challenges During: Data Collection in Smart Cities

**Joshua Gisemba Okemwa**
*Ph. D. Research Scholar*
*Department of Computer Science*
*Bhupal Nobles' University*
*Udaipur, (R.J.) [INDIA]*
*Email: okemwa@bnuniversity.ac.in*

**M. S. Deora**
*Assistant Professor*
*Department of Computer Science*
*Bhupal Nobles' University*
*Udaipur, (R.J.) [INDIA]*
*Email: deora@bnuniversity.ac.in*

## ABSTRACT

*Technology has been infused in smart city service delivery with the intention of improving the living standards of its citizens. Many governments in both developing and developed world are investing more its ideology. Smart city operations relay on collection of data processing and evaluating it in order to enable informed decision making. With huge collection of big data by sensors and other smart devices fitted in cities the challenge currently faced is how to guarantee security and privacy of data. Data faces a number of threats ranging from leakage, observation, repurposed use, misuse, unauthorized access, and duplication among others. Researchers have been advancing the algorithms that will guarantee security of innocent users and ensure the safety and privacy of their data. In this paper we have carried an investigation to measure the empirical awareness of citizens concerning privacy and security issues during data collection in smart cities; we report and analyze the findings.*

## I. INTRODUCTION

Smart city has attracted a lot of attention in recent years as it viewed as solution to increasing urbanization across the world, causing scramble for limited facilities available in the cities. There is a projection of increase in urban population up to sixty six percent per 2050. [1, 4] Internet of things and big data has played any important role in development of smart cities. Valuable insight are gotten from large quantizes of data that are collected and analyzed. [2, 1]

Governments of both developed and developing countries, feel the need of using technology to improve service delivery and citizens life. This has enhanced increase in impressing smart city ideology. [4] Indian government (GOI) for example in 2015 announced a program to develop smart cities dubbed smart city mission (SCM), a hundred cities will be developed. [5]

The creation of smart cities relay on use of sensors and smart application to ensure collection of data and service delivery. Smart city users also relay smart phones to store their data and carry out different transactions. The major challenge currently faced in smart cities is security and privacy of data during collection and processing. Various attacks are launched on data, if data is compromised it may lead to disclosure of users identify, location, health condition. This can be a big source of compromised services. [7, 1, 3]

A survey carried in 2017 noted that sources of data that are misused include: leaked data, observed data, published data, and repurposed data. To avoid this misuse of personal data, some techniques have to be applied as a countermeasure. They current measures used to handle security and privacy issues include: cryptography, block chain, biometrics, machine learning and data mining, ontology, among others. [6, 3, 1]

Researchers are currently working on advanced ways of guarantying security and privacy to smart citizens who live in the city and are subjected to use of technology in their daily activities in order to improve their quality of life.

In this paper we investigate the level of awareness of smart citizens on security and privacy issues during data collection in smart cities. The rest of the paper is organized as follows: section 2 overview of key entities. Section 3 Methodology. Section 4 Result and discussion. Section 5 Conclusion. Section 6 References.

## II. Factors Considered in Development

Renati identified that in smart city implementation contains key components that are empirically ever mentioned they include: government policy and implementations, smart city inhabitants, technology and various stakeholders. [8]

Information communication technology has continued to evolve dramatically over years. This has brought networks with great speed, capacity and increased mobility which in return as created big data. ICT has now penetrated in all areas of business and can be referred as infrastructure on its own. [9]

Government plays a role in making policies and smart city development. Its role is to improve the services offered to citizens. It uses information technology to connect different physical infrastructure that generate big data essential for decision making. [11, 9] For instance the government of India through the program smart city mission (SCM) commission development of a hundred smart cities that will be funded by the central government. [10]

Stakeholder was first defined in Stanford research institute in 1963. It referred to those groups without their support existence of an organization may cease. [13] Various definitions have been revised there after in urban set up it means those who affect or could affect a proposed development initiative. We use same interpretation for smart city development. Stakeholders include suppliers, retailers' business owners. [14]

Smart city inhabitants are citizens who will live in these cities. They are intended to have improved lives through use of technology in various operations intended to improve service delivery. Most of the operations carried by smart devices will collect data from citizens that will be analyzed and used to improve service delivery. [1, 2, 5]

These factors are key players considered when developing smart cities. In our investigation we focus to ascertain the extent of city inhabitants' awareness on security and privacy related issues in smart cities.

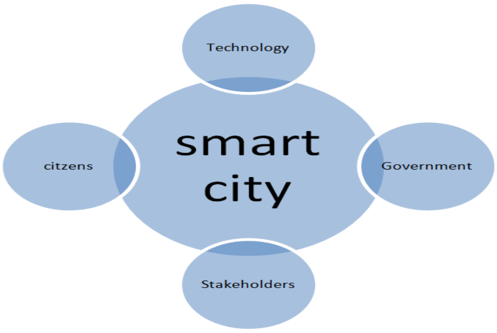

*Figure 1: The Overview this Player in Developing Smart Cities*

## III. Research Methodology

We examine the goal of our work, which is to analyze the awareness of smart city inhabitants about security and privacy issues on smart cities. The research methodology has to be efficient to achieve our goal and minimize errors. In this section we describe data collection and analysis of the data of our work.

***3.1 Data Collection:*** I designed a questionnaire to gather data from respondents of different cities. Random sampling method was used. It allowed respondents to complete the survey on their own. With advanced technology I used online based method of data collection. Google forms where created with options for respondents to tick on their response. After clicking the submission button the data was automatically collected and saved in the spreadsheet.

***3.2 Data Source:*** The data source of the research is primary data. The data was collected through a well structure self administered survey. All the areas of consideration were included in the survey questions. Questionnaire was published online and link shared among various respondents. They responded to the questions that were presented by ticking the right choice. At the end of the exercise the data was compiled for analysis.

***3.3 Sample Size:*** The current study has a sample of two hundred and twenty one smart citizens who live in cities.

***3.4 Research Design:*** Exploratory and descriptive research was used because of the nature of the research work. Based on the functioning of the stated types of research, they were efficient for the current research work.

***3.5 Data Analysis Tools:*** The tool used is statistical package for social sciences (SPSS). The statistical technique used for data analysis include, correlation, ANOVA and multiple regression analysis for finding mean and standard deviation. Microsoft word and excel were also beneficial in storage and analysis of data.

***3.6 Type of Sample:*** The sample has four main key players in smart city they include: government policy and implementation, stakeholders, smart city inhabitants and technology. The respondents from both Kenya India and other countries responded in the study.

## IV. Result and Discussion

**Table 1: Respondent's profile**

| Category | Respondent | Count | Percentage |
|---|---|---|---|
| Gender | Male | 133 | 60.3 |
| | Female | 87 | 39.3 |
| | Prefer not to say | 1 | 0.6 |
| | | | |
| Occupation | Student | 131 | 59.1 |
| | Graduate | 29 | 13.2 |
| | Employee | 39 | 17.7 |
| | Business | 14 | 6.4 |
| | Unemployed | 8 | 3.6 |
| | | | |
| Education | School level | 7 | 3.2 |
| | Under Graduate | 139 | 62.7 |
| | Post Graduate | 75 | 34.1 |
| | | | |
| Country | Kenya | 146 | 66.2 |
| | India | 55 | 24.7 |
| | Others | 20 | 9.1 |
| | | | |
| Age | 20-25 | 142 | 64.2 |
| | 26-30 | 47 | 21.1 |
| | 31-35 | 12 | 5.5 |
| | 35 - Above | 20 | 9.2 |

***Explanation:*** The number of male and female respondents is 60.3% and 39.3 respectively. It significantly shows there was male dominance in the number of respondents who responded. There is a small percentage 0.6 who preferred not to say their gender. Occupation wise students currently pursuing degrees predominantly replied to our questionnaire total of 59.1 %, this can be attributed to availability of time and being acquitted with the current technology. Kenya is leading in terms of in response with the highest age category of response being 20-25. Smart city developing and awareness is promising in future per the demographics of respondents.

***Explanation:*** The correlation measure we considered Pearson correlation denoted by (r) the representation of the number of respondents denoted by (N) and the significance (sig.)

In the figure. the correlation matrix, reveal that there was a positive and significant association between stakeholders and smart city inhabitants (r=0.252, p=0.000). There was a positive and significant association between government policy implementation and smart city inhabitants (r=0.212, p=0.001). It also reveals that there was a positive and significant association between technology advancement and smart city inhabitants (r=0.253, p=0.000).

Significance of the correlation matrix of the three associations is below significance level of (0.005) it implies that the variables are good to be used.

**Table 2 : Correlation Analysis**

**Correlations**

| | | mean_smartcityinhabitants | meanstake-holderperspective | mean_governmentpolicyandimplementation | mean_technologyadvancement |
|---|---|---|---|---|---|
| mean_smartcityinhabitants | Pearson Correlation | 1 | .252** | .212** | .253** |
| | Sig. (2-tailed) | | .000 | .001 | .000 |
| | N | 221 | 221 | 221 | 221 |
| meanstakeholder-perspective | Pearson Correlation | .252** | 1 | .240** | .066 |
| | Sig. (2-tailed) | .000 | | .000 | .330 |
| | N | 221 | 221 | 221 | 221 |
| mean_governmentpolicyandimplementation | Pearson Correlation | .212** | .240** | 1 | .088 |
| | Sig. (2-tailed) | .001 | .000 | | .191 |
| | N | 221 | 221 | 221 | 221 |
| mean_technologyadvancement | Pearson Correlation | .253** | .066 | .088 | 1 |
| | Sig. (2-tailed) | .000 | .330 | .191 | |
| | N | 221 | 221 | 221 | 221 |

**. Correlation is significant at the 0.01 level (2-tailed).

### Table 3 : Regression Analysis

| ANOVA | | | | | | |
|---|---|---|---|---|---|---|
| **Model** | | **Sum of Squares** | **df** | **Mean Square** | **F** | **Sig.** |
| 1 | Regression | 13.466 | 3 | 4.489 | 11.661 | .000$^{b}$ |
| | Residual | 83.530 | 217 | .385 | | |
| | Total | 96.995 | 220 | | | |
| a. | **Dependent Variable:** mean_smartcityinhabitants | | | | | |
| b. | **Predictors:** (Constant), mean_technologyadvancement, meanstakeholderperspective, mean_governmentpolicyandimplementation | | | | | |

***Explanation:*** The research is significant at 0.00 less than 0.05. The components identified in the investigation above contribute up to (13.4%) of variation in smart city, this implies that there are a number of more factors that can be considered in security and privacy awareness issue.

The degree of freedom is calculated by df= (n-1) n=(221-1)=220

### Table 4: Regression of coefficients

| Coefficients | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 1.872 | .362 | | 5.166 | .000 |
| | meanstakeholderperspective | .201 | .065 | .202 | 3.114 | .002 |
| | mean_governmentpolicyandimplementation | .146 | .066 | .144 | 2.207 | .028 |
| | mean_technologyadvancement | .232 | .065 | .227 | 3.584 | .000 |
| a. Dependent Variable: mean_smartcityinhabitants | | | | | | |

**Explanation:** Stakeholder explains 20.1% variation on smart city inhabitants, government policy and implementation explains (14.6%) will technology explains (23.2%) variation on smart city inhabitants. All are significant variables are very significant since it all ranges below 0.05 standard set value. We note that smart city perceive that technology has the highest source of security and privacy setback since it has the highest influence on the overall variation.

Multiple regression formula as per the analysis above:

$Y= 1.872+ 0.201X_1 + 0.146X_2 + 0.232X_3 + \mu$

Y = smart city inhabitants.

B0= constant

X1= Stakeholders perspective.

X2=Government policy & implementations.

X3=Technology advancement

μ= Error

**Table 5 : Awareness Levels**

| Awareness response | Security and privacy issues | | Taken precautions | |
|---|---|---|---|---|
| | **Count** | **Percentage** | **Count** | **Percentage** |
| **Yes** | 167 | 75.6 | 136 | 61.5 |
| **No** | 54 | 24.4 | 85 | 38.5 |
| **Total** | 221 | 100 | 221 | 100 |

**Explanation:** In this question 167 persons agreed that they are aware of security and privacy issues during data collection in smart cities equivalent to 75.6 percent while 54 persons responded NO equivalent to 24.4 percent. In the question of those who have taken precaution 136 persons responded yes equivalent to 61.5 percent while 85 persons responded no equivalent to 38.5 percent. This can be interpreted that a good percentage of respondents are aware of security and privacy issues in data collection but a lesser percentage of the people have taken precautions.

**Table 6 : Awareness Levels**

| Awareness response | Safety of smart devices in market | | Government working to secure citizens data. | |
|---|---|---|---|---|
| | **Count** | **Percentage** | **Count** | **Percentage** |
| **Yes** | 149 | 67.4 | 163 | 73.8 |
| **No** | 72 | 32.6 | 58 | 26.2 |
| **Total** | 221 | 100 | 221 | 100 |

**Explanation:** In this question 149 persons agreed the smart devices used by smart users are safe for use equivalent to 67.4 percent while 72 persons responded NO equivalent to 24.4 percent. In the question is government working to secure citizens data 163 persons responded yes equivalent to 73.8 percent while 58 persons responded no equivalent to 26.2 percent. This can be interpreted that a percentage of respondents feel that smart devices on the market are not safe but they also recognize that the government is working to enhance their safety.

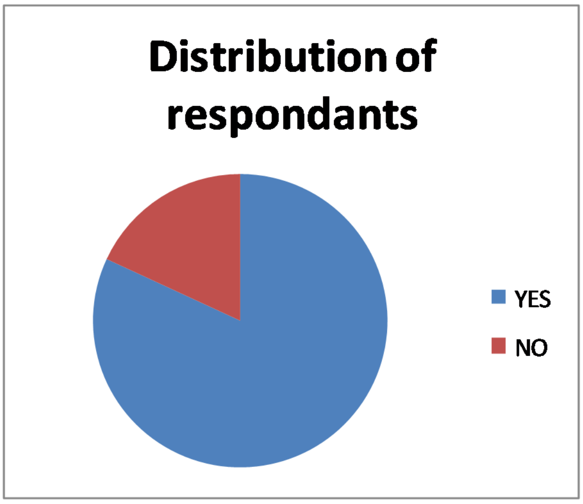

*Figure 2 : Awareness Levels Distributions of Respondents*

***Explanation:*** In this question 181 persons equivalent to 81.9 percent agreed that technology advancement is raising a lot of challenges in terms of security and privacy while 40 persons responded NO equivalent to 24.4 percent. This can be interpreted that citizens are aware that development of technology has challenges either negative or positive.

## V. Conclusion

Based on the finding of the study above we conclude that smart city inhabitants are aware of government policy and implementation, technology and stakeholders influence in privacy and security challenges in smart cities. Technology advancement has contributed to privacy and security challenges in smart cities. The citizens are aware of the policies implementation on helping to ensure that smart cities are safe when compared against the other variables the citizens believe that the contribution of government to this challenges is much lower. Stakeholders and technology are having almost equal effect on security issues in smart cities. From our analysis we conclude that the percentage effect of this variable towards security and privacy challenge is less, implying that there are many other factors out there contributing to the same problem.

## REFERENCE:

[1] Lei Cui, Gang Xie, Youyang QU. Security and Privacy in Smart Cities: Challenges and Opportunities. DOI 10.1109/ACCESS.2018.2853 985, IEEE Access

[2] Ibrahim Abaker, Targio Hashem, Victor, Badrul Anuar. The role of big data in smart city. International Journal of Information Management 36 (2016) 748–758.

[3] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Communications Magazine, vol. 55, no. 1, pp. 122–129, 2017.

[4] Sheshadri Chatterjee, Arpan Kumar Kar. Smart Cities in Developing Economies: A Literature Review and Policy Insights .International Conference on Advances in Computing, Communications and Informatics (ICACCI) 2015. pp 2335-2340.

[5] Sheshadri Chatterjee, Arpan Kumar Kar, M.P. Gupta. (2018) Success of IoT in Smart Cities of India: An empirical analysis. doi.org/10.1016/ j.giq.2018.05.002.

[6] A. M. Nia and N. K. Jha, "A comprehensive study of security of internetof-things," IEEE Transactions

on Emerging Topics in Computing, 2017.

[7] Kuan Zhang, Jianbing Ni, Kan Yang. 2017, Security and Privacy in Smart CityApplications: Challenges and Solutions. Doi 10.1109/ MCOM.2017.1600267CM. pp 122-129

[8] Renata Paola Damer. 2013 Searching for Smart City definition: a comprehensive proposal. Journal: International Journal of Computers & Technology Vol 11, No.5. pp 2544-255.

[9] Hisatsungu Tamai. (2014) Fujitsu's approach on smart cities. Fujitsu Sci. Tech. j., Vol. 50, No. 2, pp 3-10

[10] Sheshadri Chatterjee, Arpan Kumar Kar, M.P. Gupta. (2018) Success of IoT in Smart Cities of India: An empirical analysis. doi.org/10.1016/ j.giq.2018.05.002

[11] J. R. Gil-Garcia, "Towards a smart state? Inter-agency collaboration, information integration, and beyond," Information Polity, vol. 17, no. 3,4, pp. 269–280, 2012.

[12] Maysoun Ibrahim, Ali El-Zaart, Carl Adams. Stakeholders Engagement in Smart Sustainable Cities: A Proposed Model. 2017. International Conference on Computer and Applications (ICCA). Pp 342-347

[13] R. E. Freeman, "Strategic Management: A Stakeholder Approach," Pitman Series in Business and Public Policy, Pitman Publishing Inc., Pitman Books Limited, ISBN 0-273-01913-9, 1984.

* * * * *