Volume 24 (2) October 2017 ISSN 0216-423X

JABM
JOURNAL of
ACCOUNTING - BUSINESS & MANAGEMENT

Journal of Accounting – Business & Management vol. 24 no. 2 (2017) 1-15

Understanding The Correlation among Factors of Cyber System's Security for Internet of Things (IoT) in Smart Cities

Veena Jadhav*
Karippur Nanda Kumar†
Punam Dey Alias Rana‡
A. Seetharaman§
Shalini Kalia**
K. Maddulety††

Abstract

The rise of machine-to-machine (M2M) communications (hardware and software) in internet of things (IoT), let local/overseas organizations such as information systems, schools, hospitals/healthcare, libraries, environment, transportation systems, power plants, water supply, waste management, regulations enforcement, and community services shall be connected. The sharing of data and information are becoming very common among multiplatform environments. This is becoming a basic requirement in any platform to save individual data. So, authentication and regulations requirement play a vital role in safeguarding data breaches. ADANCO 2.0.1 software is used for developing structural equation modelling and testing hypothesis to conclude as follows:

1. There are few independent variables, like hardware and software, regulatory and guidelines, attack and hacking, and authentication that effect implementing a smart solution.
2. The hypothesis testing conducted in the research demonstrates the high statistical significance of the factors like security experts, education and knowledge of IT systems in various levels of age groups is required for IoT implementations in smart cities.
3. Risk-free implementation of IoT in smart cities depends on updated technology and secured communication.
4. The IoT will change the life of people and give economic benefits to the government in smart cities.

Keywords: security, IoT, authentication, data protection, reporting, MIST, structural equation model.

* Assistant Dean, S. P. Jain School of Global Management. Telephone: +6564310008. Web page: https://www.spjain.org/faculty/profiles/veena-jadhav. E-mail: veena.jadhav@spjain. org.

† Head IT S. P. Jain School of Global Management. Telephone: +6564310004. E-mail: kumar.karippurnanda @spjain.org.

‡ Post Graduate Scholar, S. P. Jain School of Global Management. Telephone: +6562724748. Web page: https://www.spjain.org. E-mail: dayrana007@gmail.com.

§ Dean, Research, S. P. Jain School of Global Management. Telephone: +6564310006. E-mail: seetha.raman @spjain.org.

** Associate Professor, Communication, S. P. Jain School of Global Management. Telephone: 91.22.61887600, Ext.: 740. E-mail: shalini.kalia@spjain.org.

†† Deputy Director, DBA, S. P. Jain School of Global Management. Telephone: +912228570277. E-mail: k.maddulety @spjain.org.

I. INTRODUCTION

The new age of increased smart-ware, mobile, smart devices, and tab sensing technologies has not only created a paradigm shift but also changed the industries like IT field, healthcare, education, tracking system, security, monitoring behavior and research. Today, we are using global positioning system (GPS) to capture location, auto-camera to document not only images but also used as a reporting tool with various individual details. It is also used as notifying alert on security and social networking sites. Digital imaging is making it possible to document travel, physical activity, and nutrition by having research participants. The IoT will change the life of people and give economic benefits to the government in smart cities.

1.1. Cyber Security

Human beings are slowly and steadily getting involved in availing services through smart devices and IoT's in the smart cities. But increasing trend of using digital services by the stakeholders are unaware that they are connected to the smart devices' which has its vulnerabilities.

A study by Hewlett-Packard showed the following (Popescul & Radu, 2016):

a) 80% of things in IoT fail to require passwords of a sufficient complexity and length.
b) 70% enable an attacker to identify valid user accounts through account enumeration.
c) 70% use unencrypted network services.
d) 60% raise security concerns with their user interfaces.

1.2. Smart City

Many cities around the world are seeking to become a smart city, using networked, digital technologies and urban big data to tackle a range of issues, such as improving governance and service delivery, creating more resilient critical infrastructure, growing the local economy, becoming more sustainable, producing better mobility, gaining transparency and accountability, enhancing quality of life, and increasing safety and security. In short, the desire is to use digital technology to improve the following (Kitchin, 2016):

a) Lives of citizens.
b) Finesse city management.
c) Create economic development.

1.3. Internet of Things (IoT)

The internet of things (IoT) is digital machines, objects, animals or people that can transfer information over a network without requiring human-to-human or human-to-computer interaction, e.g. cameras, home security, light system, speakers, watch, phones, tabs, fitness device etc.

As the internet of things (IoT) and the web of things (WoT) are becoming a reality, their interconnection with mobile phone computing is increasing. Mobile phone integrated sensors offer advanced services, which when combined with web-enabled real-world devices located near the mobile user (e.g., body area networks, radio-frequency identification tags, energy monitors, environmental sensors, etc.), have the potential of enhancing the overall user knowledge, perception and experience, encouraging more informed choices and better decisions (Kamilaris & Pitsillides, 2016).

1.4. Research Objectives and Questions

The objective of this research aims to establish the factors influencing which effects the adoption of IoT in smart cities or reaping IoT benefits in smart cities without compromising security related to technology and data breaches.

The research aims to answer the following questions:

a) How can a near perfect environment- be achieved by implementing proper regulation and guideline with technology advancement in the age of the internet of things (IoT) and near future artificial intelligence (AI)?
b) Do regulations are a burden, or it is a competitive advantage for those who believe in IT security?
c) How shall a standardized model approach be taken with the advancement of technology so that we shall be able to protect IoT stakeholders?
d) How education and control from regulatory bodies/government organization shall help to create a better smart city in future?

II. REVIEW OF LITERATURE AND RESEARCH STRUCTURE

2.1. Technology

Frost and Sullivan (2014) latest report 'analysis of the internet of things market in the Asia Pacific' expects the internet of things (IoT) market to be one of the fastest-growing segments in the Asia Pacific technology industry. Total Asia Pacific spending on IoT is forecast to be USD9.96 billion in 2014 and will continue to grow at a CAGR of 34.1% to reach USD57.96 billion by 2020. So, technology in future shall work more towards effective secured communication option in hardware level. The software giant sees IoT, not as a futuristic, aspirational technology trend. The internet of things (IoT) has following intrinsic functional characteristics (Katole et al., 2015):

a) Sensing.
b) Network of networks.
c) Intelligent processing.

Quantifying the value, volume and variety relative to the costs of veracity become of paramount importance to evaluate the effectiveness of big data investments for now and future (Abbasi et al., 2016). The standard uses RESTful protocol for building its interfaces, to keep it as simple as possible and to encourage its adoption (Ionescu, 2015).

Based on the above literature the following research questions arise:

a) In smart cities do rules and regulations play a positive role in implementing IoT?
b) Does a proper implementation hardware and software and authentication have a positive relationship with rules and regulations of IoT in smart cities?

Technological factors affecting businesses all over the world, either a hardware or software change to support business needs, Decisions regarding security are taken with more confidence and with more results when the whole security context is known (Ionita & Patriciu, 2016).

Data confidentiality is a key issue in Information Technology not only in banking and financial services companies but also at the personal level where human being are getting connected to IoT applications in smart cities now and then.

The Federal Financial Institutions Examination Council (FFIEC) provides detailed examination requirements around information security in its Information Security IT Booklet and Supervision of Technology Service Providers IT Booklet (Reck, 2015).

In a study done by McAfee, it is estimated that the global economy loses over $400 billion annually due to cybercrime. Apart from financial loss, it is also estimated that roughly 200,000 jobs have been lost due to a ripple effect from these cybercrimes (Raju & Verhaart, 2016). Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based

upon internationally accepted best practices and standards and utilizing privacy and security technologies (Shackelford & Kastelic, 2015). The SWOT analysis shall be used as a strategic tool to identify the gap between existing resources and pre-requisites of smart city transformation (Sarkar & Viramgami, 2016).

Based on the above literature the following research questions arise:

a) Do attack and hacking have the operation of IoT in smart cities?
b) Do attack and hacking have relation with hardware and software?

2.2. Data Protection and Authentication

IoT in smart cities not only has the same security issues as sensor networks, mobile communications networks and the Internet but also has its specialties such as privacy issues, different authentication and access control network configuration issues and information storage and management and so on. Data and privacy protection are one of the key application challenges of IoT.

There are two major security issues in the transmission of data process (Jing et al., 2014) namely risk of IoT security and implementation of the network functions. To safeguard personal data, data minimization should also be practiced; that is, the data collected should be limited to only that which is necessary for the effective functioning of the device and the application (Maras, 2015).

Authentication is used for data protection, device authentication and data exchange between different applications for a long time. Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database.

Based on the above literature the following research questions arise:

a) Should IoT in smart cities and data sharing be controlled by proper authentication techniques?
b) Should authentication of IoT in the smart city be able to protect stakeholders from attack and hack positively?

2.3. Layers in Smart Cities

As per as our findings, we will divide IoT in smart cities into three layers (Jing et al., 2014) namely Perception layer, Transportation layer and Application layer. IoT must ensure the security of all the three layers mentioned above. Authentication, access control, and digital signature play an important role in this area.

2.4. Standardization

In the world of IoT and AI, standardization plays an important role in securing personal information and data. Information and communications technology (ICT) is increasingly used in governmental and regulatory processes. With the development of the 'Internet of Things' researchers speak about the birth of the 'smart city'. But, open problems remain in many areas, such as security and privacy protection, network protocols, standardization, identity management, trusted architecture etc. (Li et al., 2016). However, the role of ICT is very crucial in implementing IoT in smart cities to bring standardization in the area of implementing the technology. The practice of regulation and guidelines are becoming an increasingly important feature of the present day with the changing technology. More of e-governance is required in smart cities with changing time and technology (Kennedy, 2016).

Legal liability frameworks for the bad decisions of automated systems will have to be established by governments, companies, and risk analysts, in consort with insurers (Skaržauskienė & Kalinauskas, 2012). Intellectual property (IP) rights are also becoming

very important to protect company's rights in the field inventions, trademarks, industrial designs and geographical indications. Various research demonstrates not only the need for developers to begin considering secure coding, but also the need for IT management to encourage and implement secure coding principles in their development lifecycle (Grover et al., 2016).

Sharing personal information smart environments, applications and sharing of data are increasing day by day. This creates a need for Web to provide appropriate information/awareness to the stakeholders about the details of processed information (Siddiqui & Lee, 2016).

Based on the above literature the following research question arises:

a) Do standardization, rules and regulations; education etc. have positive effects on the security of IoT in smart cities?

By considering above literature from 2.1 to 2.4 i.e. the technology, data protection authentication, layers in smart cities and standardization we can arrive at the following nine hypotheses:

H_1: regulations and guidelines etc. have positive effect on the security of IoT in smart cities.

H_2: regulations and guidelines etc. have positive effect on authentication.

H_3: regulations and guidelines etc. has positive effect on software and hardware.

H_4: authentication has positive effect on the security of IoT in smart cities.

H_5: attack and hacking do not stop the operation but it leads to huge loss of money in smart cities.

H_6: attack and hacking have correlation with authentication given to IoT in smart cities.

H_7: attack and hacking have correlation with hardware and software used in IoT in Smart cities.

H_8: proper implementation of hardware and software has a positive relationship with IoT in smart cities.

H_9: authentication has positive correlation with implementation/installation of hardware and software.

2.5. Deriving Benefits

Smart information has become a vital resource with the deployment of heterogeneous smart sensors and devices over the Internet. The emergence of wireless sensor networks within smart environment aims to provide "anytime-anywhere" computing. Availing and sharing of information come with various internal and external threats as mentioned below (Siddiqui & Lee, 2016).

To reap the benefits of all the latest advancement of the technology and avoid threats, stakeholder must follow various IT rules and regulations. There is no comprehensive federal statute that protects the privacy of personal information held by the public sector. Instead, federal law tends to employ a sectoral approach to the regulation of personal information" (Halepoto et al., 2015).

Universities are under increased pressure to produce graduates with better security knowledge and skills, particularly emerging cybersecurity skills (Harris & Patten, 2015). The Internet of Things currently connects tens of billions of devices worldwide and has the potential to generate trillions of dollars in economic opportunity. Increased connectivity can empower consumers in nearly every aspect of their daily lives, including in the fields of agriculture, education, energy, healthcare, public safety, security, and transportation (Halepoto et al., 2015).

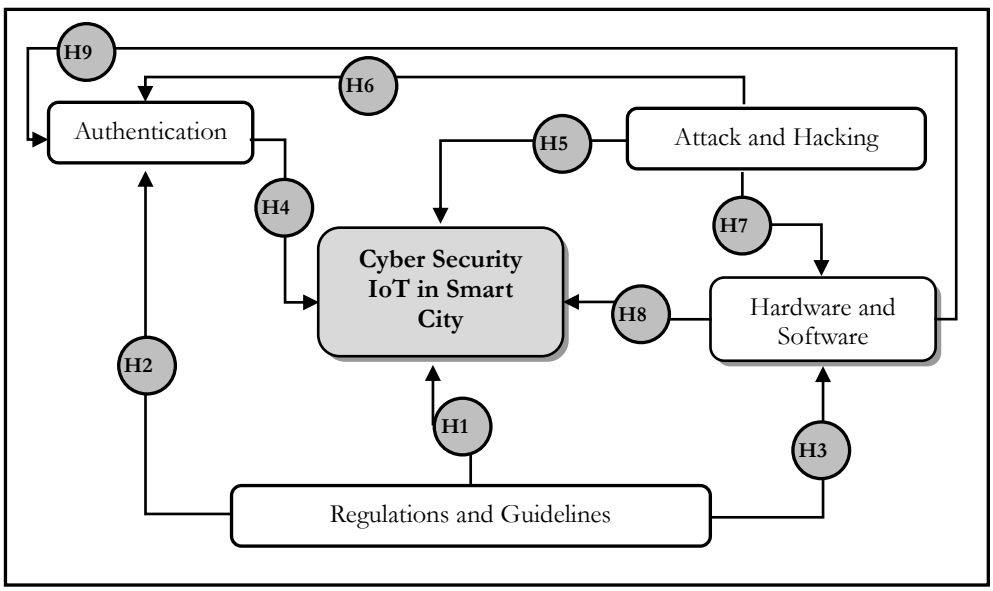
To understand the role of IoT application in smart cities, a clear vision is required. Smart cities conceived as ecosystems should provide policymakers with some practical guidelines to integrate soft and hard domains and the evolutionary process of emergence of the future smart city. Three areas for smart government appear (Rochet & Pinzón Correa, 2016) namely economic development, a vibrant political life and supporting open innovation.

III. RESEARCH METHODOLOGY AND FRAMEWORK

The primary research was conducted comprising specific interviews, surveys, questionnaires etc. and the secondary research was done based on the literature review from Google scholars, pro-quest and ISI journals. The primary data was collected through an online questionnaire, and the secondary data was collected from 45+ academic journals in Google scholars, pro-quest etc. explaining the cyber security on IoT applications in smart cities.

Figure 1

Research Framework



3.1. Research Questionnaire

Below are the questions prepared to identify the effect of independent variables on dependent variable for "a study of cyber-system's security for internet of things (IoT) in smart cities" and independent variables are authentication, hardware, and software, attack and hacking, regulations and guidelines, benefits of smart cities.

3.2. Data Collection Method

The questionnaire was distributed among people who are living in smart cities and uses IoT applications now and then such as information technology, dealing with information technology, finance, medical/healthcare, education, retails etc.

Before circulating the online questionnaire, it was pre-tested to identify new independent variables that could influence. A study of cyber-system's security for the internet of things (IoT) in smart cities.

3.3. Profile of Respondents

The online questionnaire was sent to the participants using various modes like an email invitation, an invitation through LinkedIn, Facebook and WhatsApp. A total of 325 ++ responded to the survey using google forms. This was made possible with the help of a network consisting of two representatives from each region. The detailed distribution of the profile of the participants is provided in table below.

Below are the details of demographics of the respondents (n= 307) with respect to industry, professional level, region, qualification and age group:

Table 1
Demographics of the Respondents

	Items	Measure	Frequency	Percentage
1.	**Industry**	Information Technology	115	44.60%
		Dealing with Information Technology	30	11.60%
		Finance	28	10.90%
		Medical/Healthcare	20	7.80%
		Education	23	8.90%
		Retails	8	3.10%
		Others	34	13.20%
2.	**Professional Level**	Senior Level	77	25.08%
		Middle Level	156	50.81%
		Junior Level	74	24.10%
3.	**Region**	America	34	11.07%
		Europe	23	7.49%
		Asia Pacific/Middle East	236	76.87%
		Africa	14	4.56%
4.	**Qualifications**	Diploma	43	14.01%
		Bachelor's degree/Equations	112	36.48%
		Master's degree/Equations	126	41.04%
		Doctorate degree	26	8.47%
5.	**Age Groups of Respondents**	18-24	34	11.07%
		25-34	99	32.25%
		35-44	124	40.39%
		45-54	33	10.75%
		55-64	12	3.91%
		Above 64	5	1.63%

IV. DATA ANALYSIS

The primary data that was collected through the online survey questionnaire and modeled using the ADANCO statistical package or PL-SEM which is a structural equation modeling tool for modeling variance-based structural equations, proposed hypotheses for constructing a research framework.

4.1. Construct Reliability

The composite reliability is an estimate of the reliability of sum scores pertaining to a reflective measurement model.

Table 2
Construct Reliability

	Construct	Dijkstra-Henseler's rho (ρ_A)	Jöreskog's rho (ρ_c)	Cronbach's alpha(α)
1.	**Smart City & IoT**	0.6709	0.8043	0.6744
2.	**Regulations & Guidelines**	0.7449	0.8503	0.7365
3.	**Authentication**	0.6320	0.8446	0.6320
4.	**Attack & Hacking**	0.7249	0.8321	0.6966
5.	**Hardware & Software**	0.6166	0.7761	0.5929

4.2. Convergent Validity

Convergent validity, a parameter often used to refer to the degree of two measures of constructs that theoretically should be related, are in fact related. The below-mentioned table shows convergent validity for the model established from the research and their relationship amount the identified variables.

Table 3
Convergent Validity

	Construct	Average Variance Extracted (AVE)
1.	**Smart City & IoT**	0.5080
2.	**Regulations & Guidelines**	0.6548
3.	**Authentication**	0.7310
4.	**Attack & Hacking**	0.6249
5.	**Hardware & Software**	0.5375

4.3. Discriminant Validity

The discriminant validity or divergent validity tests, whether concepts or measurements that are not supposed to be related are, in fact, unrelated. The below-mentioned table shows discriminant validity for the model established from the research and their relationship amount the identified variables.

Table 4
Discriminant Validity

	Construct	Smart City & IoT	Regulations & Guidelines	Authen-tication	Attack & Hacking	Hard. & Software
1.	**Smart City & IoT**	0.5080				
2.	**Regulations & Guidelines**	0.1218	0.6548			
3.	**Authentication**	0.2209	0.1019	0.7310		
4.	**Attack & Hacking**	0.1092	0.1392	0.1401	0.6249	
5.	**Hardware & Software**	0.2138	0.0637	0.1043	0.0651	0.5375

Squared correlations; AVE in the diagonal.

4.4. Structural Model

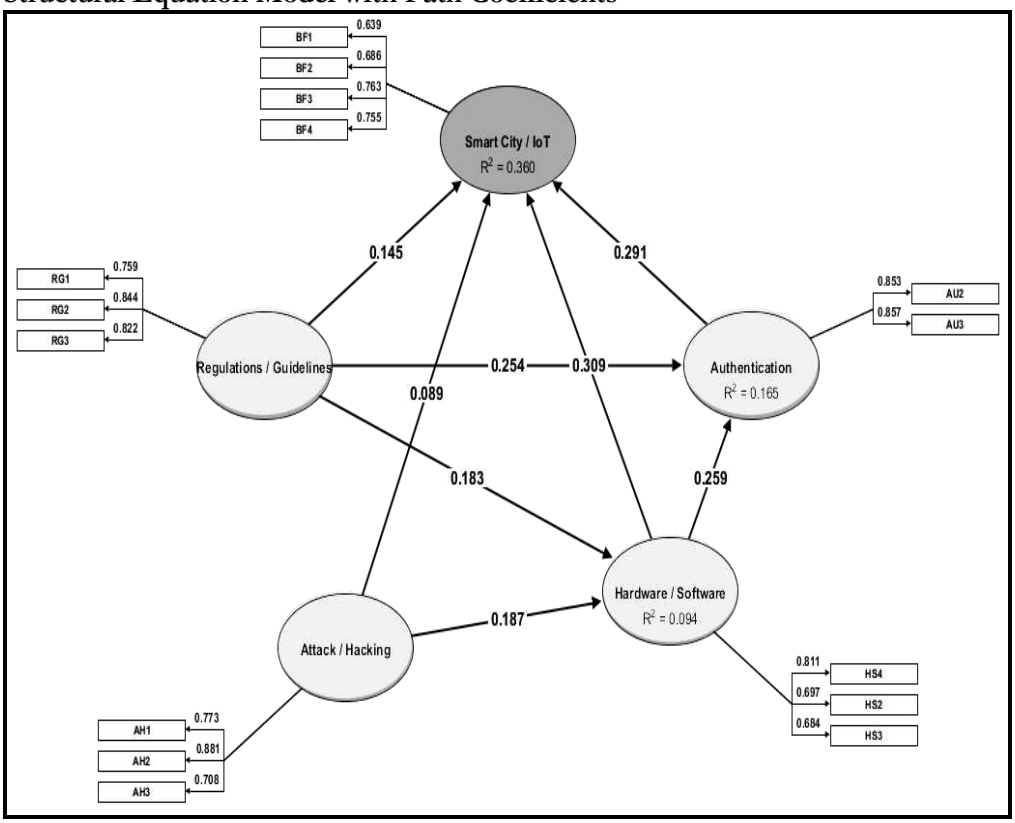
A structural model is given below under path analysis.

4.5. Path Analysis

A structural equation modeling (SEM) is path analysis, or a causal modeling in which single indicators are used in the causal model for each variable. The strength of each path is calculated as a product of the path coefficient along that path.

4.5.1. Model Creation

Figure 2
Structural Equation Model with Path Coefficients



4.6. Overall Model

4.6.1. Goodness of Model Fit (Saturated Model)

Goodness of model fit is measured with SRMR (Standardised Root Mean Square Residual) for saturated model and estimated model are .08 and .09 respectively.

V. HYPOTHESIS TESTING

5.1. Outcome of Hypotheses Testing

Insert Table 5 here.

VI. RESEARCH FINDINGS

We identified nine hypotheses, and the path coefficient for all the hypotheses that have been identified is strongly accepted. The hypothesis (6), i.e. attack/hacking → authentication seems to have less impact on an adaptation of IoT in smart cities. Following is the detailed explanation of the hypothesis defined.

1. Regulations/guidelines → smart city/IoT (1): the impact of regulations and guideline on smart cities and IoT applications is quite evident from the data collected during the survey. It shows that the regulations and guideline has a high impact on smart cities with t-value= 4.5102. Comparing the table above it show CI>99% (β= 0.2891 and p= 0.0000) is highly accepted.

Table 5
Total Effects Inference

	Effect	Original Coefficient (β)	Standard Bootstrap Results					Percentile Bootstrap Quantiles				Support
			Mean Value	Standard Error	t-value	p-value (2-sided)	p-value (1-sided)	0.5%	2.5%	97.5%	99.5%	
1.	Regulations/Guidelines → Smart City/IoT	0.2891	0.2931	0.0641	4.5102	0.0000	0.0000	0.1261	0.1585	0.4201	0.4562	Yes
2.	Regulations/Guidelines → Authentication	0.3011	0.3066	0.0595	5.0646	0.0000	0.0000	0.1470	0.1856	0.4158	0.4589	Yes
3.	Regulations/Guidelines → Hardware/Software	0.1826	0.1911	0.0598	3.0555	0.0023	0.0012	0.0322	0.0750	0.3097	0.3437	Yes
4.	Authentication → Smart City/IoT	0.2906	0.2845	0.0649	4.4808	0.0000	0.0000	0.1269	0.1584	0.4054	0.4410	Yes
5.	Attack / Hacking → Smart City/IoT	0.1606	0.1691	0.0693	2.3171	0.0207	0.0104	0.0280	0.0337	0.2995	0.3333	Yes
6.	Attack/Hacking → Authentication	0.0484	0.0504	0.0227	2.1368	0.0329	0.0164	0.0036	0.0115	0.0984	0.1200	Yes
7.	Attack/Hacking → Hardware/Software	0.1871	0.1916	0.0684	2.7363	0.0063	0.0032	0.0179	0.0523	0.3150	0.3442	Yes
8.	Hardware/Software → Smart City/IoT	0.3845	0.3813	0.0633	6.0747	0.0000	0.0000	0.2025	0.2571	0.5038	0.5335	Yes
9.	Hardware/Software → Authentication	0.2588	0.2596	0.0581	4.4517	0.0000	0.0000	0.1129	0.1445	0.3711	0.4070	Yes

2. Regulations/guidelines → authentication (2): the impact of regulations and guideline on authentication is the highest as per as the research record. It shows that the regulations and guideline has a higher impact on smart cities/IoT applications if it is not controlled by proper authentication system (t-value= 5.0646). Comparing the table above it shows CI>99% (β= 0.3011 and p= 0.0000) is highly accepted.
3. Regulations/guidelines → hardware/software (3): the impact of regulations and guideline on hardware and software is high as well. It shows that the regulations and guideline have an impact on hardware/software that we shall use to implement IoT applications in smart cities. The t-value= 3.0555 from the research data and comparing the table above it shows CI>99% (β= 0.1826 and p= 0.0012) is highly accepted.
4. Authentication → smart city/IoT (4): the data show that the impact of authentication on smart cities and IoT applications is also very high. It shows that the regulations and guideline has a high impact on smart cities with t-value= 4.4808. Comparing the table above it show CI>99% (β= 0.2906 and p= 0.0000) is highly accepted.
5. Attack/hacking → smart city/IoT (5): the date received from the research shows that the t-value= 2.3171and comparing the table above it shows CI>97% (β= 0.1606 and p= 0.0104) is accepted too.
6. Attack/hacking → authentication (6): the data show that the impact of attack and hacking on authentication of IoT applications in smart cities is accepted and high. It shows the impact on authentication with t-value= 2.1368. Comparing the table above it shows CI>97% (β= 0.0484 and p= 0.0164) is quite significant. So, authentication plays an important role in controlling attack and hacking in smart cities/IoT applications.
7. Attack/hacking → hardware/software (7): the impact of the attack and hacking on hardware and software is quite evident from the data collected during the survey. It shows that the attack and hacking shall be controlled by selection of proper hardware and software. Comparing the data from the analysis it shows that the t-value= 2.7363 and CI>99% (β= 0.1871 and p= 0.0032) is highly acceptable.
8. Hardware/software → smart city/IoT (8): the data show that the impact of hardware and software in smart cities is accepted to the highest level. It shows the impact on authentication with t-value = 6.0747. Comparing the table above it show CI>99% (β= 0.3845and p= 0.0000) is very significant. So, hardware and software play a very import role in the life of stakeholder in smart cities.
9. Hardware/software → authentication (9): the data show that the impact of hardware and software on the authentication of IoT application in smart cities has a high impact. It shows that the stakeholders are getting aware of authentication to protect personal information. But, more education is required to align people to understand technology and take advantage of it. The t-value= 4.4517 and CI>99% (β= 0.2588 and p= 0.0000) is highly accepted.

VII. CONTRIBUTIONS

This research investigated the factors influencing the cyber systems security of IoT in smart cities and its adoption.

1. Do the factors like hardware and software, authentication, regulatory and guidelines, and attacks are very imported while implementing a smart solution?

2. Security experts, education system at the various level of society and knowledge about transparency with authentication shall help stakeholders to reap the risk-free benefit of IoT applications?
3. How to handle risk-free implementation of fast moving of IT technology?
4. How the industries like healthcare, education, childcare etc. shall get benefited from the implementation of IoTs in smart cities.

The data clearly highlights following answers based on above questions:

1. First, our research findings show that there are few independent variables, like hardware and software, regulatory and guidelines, attack and hacking, and authentication effects the implementing a smart solution.
2. Second, the hypothesis testing conducted in the research demonstrates the high statistical significance of the factors like security experts, education and knowledge of IT systems in various levels of ages groups is required for IoT implementations in smart cities.
3. Third, the detail of the research questionnaires is shared among professional in IT industry and compared with the various scholar journals. It is evident from the data derived from the questionnaire that for a risk-free implementation of IoT in smart cities depends on updated technology and secured communication.
4. Finally, the IoT will change the life of people and give economic benefits to the government in smart cities.

VIII. FUTURE SCOPE OF RESEARCH

This article tries to highlight the benefit that human beings can have in using IoT by smart cities. How e-governance/regulatory bodies, ICT and self-awareness can help to reap the full benefits of technology in smart cities, but it doesn't highlight the future scope of cyber security in the field of artificial intelligence (AI).

As threat from cyber security increasing in smart cities with increasing internet of things/e-services applications. A new approach and better solutions are needed. Yahoo! revealed the largest known security breach to date, which compromised over 1 Billion accounts, only months after it reported a separate breach involving 500 million users. These intrusions could take years to resolve and cost millions of dollars.

IX. CONCLUSIONS

Internet of Things (IoT) is not only important and closer to a human being but is also changing the lifestyle in smart cities. It is also changing an average person to a smart individual.

The impact of regulations and guideline on smart cities and IoT applications is quite evident from the data analysis. It shows that the regulations and guideline has a high impact on smart cities with β= 0.289, p=0.0000 and t-value= 4.5102. The impact of regulations and guideline on authentication is the highest as per the research record. It shows that the regulations and guideline has a higher impact on smart cities/IoT applications if it is not controlled by proper authentication system. It is evident with β= 0.3011, p= 0.0000 and t-value= 5.0646 is highly accepted. The results also show that the regulations and guideline haves impact on hardware/software that we shall use to implement IoT applications in smart cities. β= 0.1826, p= 0.0012 and t-value= 3.0555. The authentication of smart cities and IoT applications is also very high because β= 0.2906 p= 0.0000 and t-value= 4.4808. The analysis also shows that: attack and hacking effects on smart city/IoT, it is evidenced β= 0.1606 and p= 0.0104 and t-value= 2.3171. The analysis shows that the impact of the attack and hacking on

authentication of IoT applications in smart cities is accepted and high it is evidenced β= 0.0484, p= 0.0164 and t-value= 2.1368. The impact of the attack and hacking on hardware and software is quite evident from the analysis β= 0.1871, p= 0.0032 and t-value= 2.7363. The impact of hardware and software in smart cities is accepted to the highest level because β= 0.3845, p= 0.0000 and t-value= 6.0747. The impact of hardware and software on the authentication of IoT application in smart cities has a high impact β= 0.2588, p= 0.0000 and t-value= 4.4517.

Smart cities and IoTs is helping a human being in all the fields like healthcare, tracking system, retail market, parenting, weather and environment, alert system and notifications, politics etc. It is also changing the lifestyle of human beings, but it comes with all of the security issues which shall be handled time to time with change technology.

Though the technology is available, IoT in smart cities has not been implemented effectively because we have made stakeholders more IT educated, aware of legal frameworks, ethical process, security and social fields. Most importantly, e-governance and regulatory authorities will play a great role in protecting individuals from data breaches.

As the significance of IoT grows in government and the corporate world in smart cities, concerns about the privacy policy, data breaches, hacking, and security are also increasing. With IoT connected devices being deployed every day, we must re-visit regulation and guidelines, security measure, and latest technology hacks before implementing one. IoT solutions must be reviewed in context with the purpose of stakeholders using it and must be secured from the initial stage itself with a holistic strategy while adding value to the smart cities.

A crucial component of IoT in a smart city is to ensure security, safety and privacy its economic and societal benefits. There is a dire need to create a robust framework with a proper regulation and guidelines for projecting stakeholder's rights and their data. Even stakeholders must educate themselves, follow guidelines and abide by rules and regulations formed by government/regulatory bodies for making our city not smart but also beautiful.

REFERENCES

Abbasi, A., Sarker, S., & Chiang, R. H. L. (2016, February). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems, 17*(2), 1-32. Retrieved from https://search-proquest-com.spjain.idm.oclc.org/docview/1773772634?accountid=162730.

Frost & Sullivan (2014, September 23). *Analysis of the Asia-Pasific internet of things market*. Retrieved from https://store.frost.com/analysis-of-the-asia-pacific-internet-of-things-market.html.

Grover, M., Cummings, J., & Janicki, T. (2016, April). Moving beyond coding: Why secure coding should be implemented. *Journal of Information Systems Applied Research, 9*(1), 38-46.

Halepoto, I. A., Sahito, A. A., Uqaili, M. A., Chowdhry, B. S., & Riaz, T. (2015, February 17-19). *Multi-criteria assessment of smart city transformation based on SWOT analysis*. Paper presented at 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 1-6. IEEE.

Harris, M. A., & Patten, K. P. (2015). Using bloom's and webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum. *Journal of Information Systems Education*, *26*(3), 219-234. Retrieved from https://scholar.google.co.in/citations?user=6ku7l6kAAAAJ&hl=en#d=gs_md_cita-d&p=&u=%2Fcitations%3Fview_op%3Dview_citation%26hl%3Den%26user%3D6ku7l6kAAAAJ%26citation_for_view%3D6ku7l6kAAAAJ%3Ae5wmG9Sq2KIC%26tzom%3D-330.

Ionescu, A. (2015). Standard interfaces for open source infrastructure as a service platforms. *Informatica Economica, 19*(4), 68-80. Retrieved from http://dx.doi.org.spjain.idm.oclc.org/10.12948/issn14531305/19.4.2015.06.

Ionita, M. G., & Patriciu, V. V. (2016, September). Secure threat information exchange across the internet of things for cyber defense in a fog computing environment. *Informatica Economica*, *20*(3), 16-27. Retrieved from http://revistaie.ase.ro/content/79/02%20-%20Ionita,%20Patriciu.pdf. Doi: 10.12948/issn14531305/20.3.2016.02.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives & challenges. *Wireless Networks*, *20*(8), 2481-2501. Retrieved from http://dx.doi.org.spjain.idm.oclc.org/10.1007/s11276-014-0761-7.

Kamilaris, A., & Pitsillides, A. (2016). Mobile phone computing and the internet of things: A survey. *IEEE Internet of Things Journal, 3*(6), 885-898. Retrieved from http://dx.doi.org.spjain.idm.oclc.org/10.1109/JIOT.2016.2600569.

Katole, B., Suresh, V., Gosavi, G., Kudale, A., Thakare, G., Yendargaye, G., & Kumar, C. P. (2015). The integrated middleware framework for heterogeneous internet of things (IoT). *Intelligence*, *4*(7), 173-177.

Kennedy, R. (2016). E-regulation and the rule of law: Smart government, institutional information infrastructures, and fundamental values. *Information Polity, 21*(1), 77-98. Doi: http://dx.doi.org/10.3233/IP-150368.

Kitchin, R. (2016, January 28th). *Getting smarter about smart cities: Improving data privacy and data security*. Dublin, Ireland: Data Protection Unit, Department of the Taoiseach on behalf of the Government Data Forum.

Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research*, *26*(2), 337-359. Retrieved from https://search-proquest-com.spjain.idm.oclc.org/docview/1775395733?accountid=162730.

Maras, M. H. (2015). Internet of things: Security and privacy implications. *International Data Privacy Law, 5*(2), 99-104. Retrieved from http://dx.doi.org.spjain.idm.oclc.org/10.1093/idpl/ipv004.

Popescul, D., & Radu, L. D. (2016). Data security in smart cities: Challenges and solutions. *Informatica Economica*, *20*(1), 29-38. Retrieved from http://dx.doi.org.spjain.idm.oclc.org/10.12948/issn14531305/20.1.2016.03.

Raju, R., & Verhaart, M. (2016, July 11-13). *Impact of Cybercrime on SMEs*. Paper presented at the incorporating the 7th annual conference of CITRENZ 2016 & the 29th annual conference of the National Advisory Committee on Computing Qualifications Wellington, New Zealand (pp. 108-109). Retrieved from http://www.citrenz.ac.nz/2016-proceedings/.

Reck, R. (2015, November). The changing information security landscape. *Mortgage Banking, 76*(2), 74-76, 78-79. Retrieved from https://search-proquest-com.spjain.idm.oclc.org/docview/1736783738?accountid=162730.

Rochet, C., & Pinzón Correa, J. D. (2016). Urban lifecycle management: A research program for smart government of smart cities. *Revista De Gestão e Secretariado, 7*(2), 01-20. Retrieved from https://search-proquest-com.spjain.idm.oclc.org/docview/1818309268?accountid=162730.

Sarkar, D. & Viramgami, R. (2016, December). Smart cities: A study of prospects beyond information and communication technology (ICT). *International Advanced Research Journal in Science, Engineering & Technology (IARJSET), 3*(12), 36-41. Retrieved from http://www.iarjset.com/upload/2016/december-16/IARJSET%207.pdf.

Shackelford, S. J., & Kastelic, A. (2015, May 12). Toward a state-centric cyber peace? Analyzing the role of national cybersecurity strategies in enhancing global cybersecurity. *NYUJ of Legislation & Public Policy, 18,* 895-984.

Siddiqui, I. F., & Lee, S. U. (2016, October). Access control as a service for information protection in semantic web based smart environment. *Journal of Internet Computing & Services (JICS), 17*(5), 9-16. Retrieved from http://dx.doi.org/10.7472/jksii.2016.17.5.09.

Skaržauskienė, A., & Kalinauskas, M. (2012). The future potential of internet of things. *Social Technologies* (MRU), *2*(1), 102-113.