IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

ISSN: 2664-9519 (Online); Vol. 1, Issue 2, November 2019

A Novel Framework for Cyber Secure Smart City

Abeer Iftikhar Tahirkheli

[1] Armed Forces Institute of Cardiology, National Institute of Heart Disease, Rawalpindi

* Corresponding Author: Abeer Iftikhar, abeer_iftikhar@yahoo.com

Received; 20 September, Revised; 30 October Accepted; 10 November

Abstract: This paper presents a novel theoretical framework by taking numerous viewpoints to Governing the cyber secure smart cities. The paper also identifies suitable approaches and frameworks to transform the legacy of urban governess into a new concept of governing cyber-secure smart cities. The analysis is purely based on an extensive literature review, proposes a framework to provide a realistic blueprint and suggests the implementation of secure smart Governance at city level for underdeveloped countries that possess meager resources and densely populated metropolitan cities. Association between safe smart city architecture and a legacy smart city system is analyzed. The proposed framework focus on cybersecurity illustrates implementing cyber secure-smart cities with all elements and information and communication technologies based systems rather make a mandatory part of any transformation of a traditional cities concept into a secure smart city.

Keywords: Smart City, Cyber Security, ICT Infrastructure, Urban Centers, E-Government, Smart Governance, Frameworks, Public Key Encryption

1. Introduction

This research provides an in-depth understanding of the nascent concept of secure smart cities through embedding the cybersecurity protocols and systems into the new integrated architecture. This paper attempts to analyze association among safe smart city architecture and legacy smart city systems. A new concept of secure smart Governance is transforming an old legacy city into a smarter city. Secure smart cities have gained importance as a means of making Information and Communication Technology (ICT) enabled services and applications available to the citizens, and authorities that are part of a city system [1-8].

A smart city can be defined as a "Collection of smart computing technologies applied to critical infrastructure components and services, including city administration, education, healthcare, public safety, real estate, transportation, and related utilities with more intelligent processes and interconnected networks" [9]. Batty, et al. [10] defines "City is considered to be declared a smart city where investments in human, social capital and traditional (transport) and modern ICT communication infrastructure, fuel sustainable economic growth and a high quality of life, with a visionary management of available natural resources, through participatory governance". Since last decade, the cities are in transformation process from legacy system into automated smart cities in areas like serving citizens, buildings, traffic systems but this concept is getting improved enabling us to monitor, control, recognize, comprehend and plan future cities to improve efficacy, impartiality, economical equity and quality of life for its citizens in real-time [11].

This paper emphasized the provision of adequate security policy/framework in parallel to the implementation of cyber-secure smart cities. This gap has been learned from the literature review. Mostly in academia, more emphasis being done for the implementation and development of infrastructures of the smart cities whereas the security framework is not catered religiously. Security is the nucleus of a secure smart city initiative. In a cybersecurity context, this paper provides an inclusive security policy and standards related to different operation layers such as data link, application, network, and physical layer, to achieve coherence and unique security along with all the data being produced, generated and methodically evaluated will be protected via public key encryption [12]. Figure 1 presents the cardinals of the smart city.

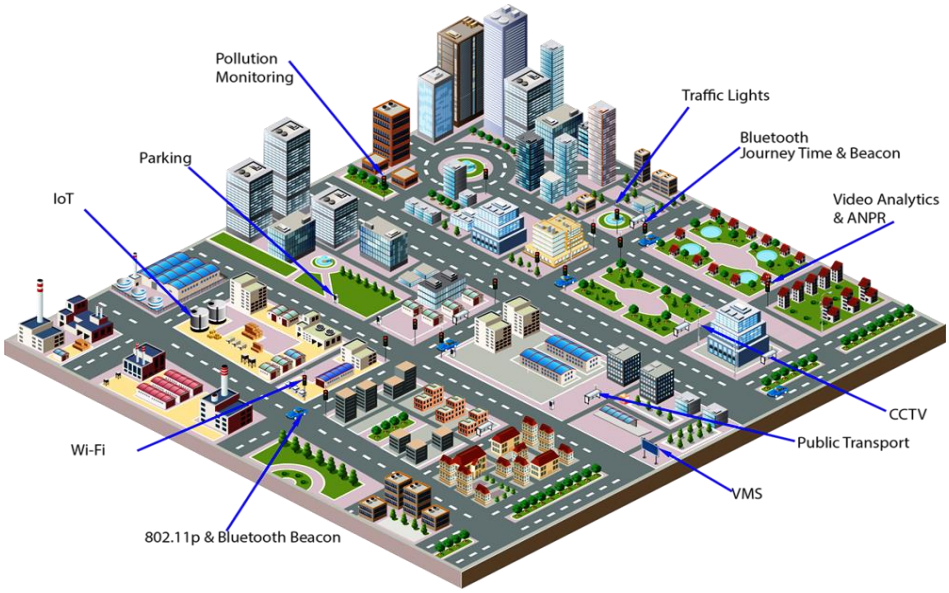

Figure 1. Cardinals of the Smart City [6].

This paper highlights major trials to its implementation and an absence of any standard makes it quite challenging and hence there is an overwhelming requirement of development of a global framework that caters to this scenario. The objective of this paper to study the impact of the synergy of secure and smart systems on future urban centers, define the smart city and measure fundamental characteristics using performance factors to comprehend smart city such as smart Governance, smart citizens, smart economy, and smart mobility. This model builds a workable framework for implementing secure smart Governance through improved Socio-Techno Synergy. A pilot/prototype model will be deployed in the capital city with the proper cloud-based application along with the android based applications to ascertain the futuristic prospects, and finally to devise a cyber-security model for the smart city [13].

This paper is organized into four sections including the existing framework, proposed framework, simulation and evaluation, and finally recommendations and conclusion.

2. EXISTING FRAMEWORKS

2.1. Smart City

Frameworks are used for the creation of a suitable and workable phenomenon for the under-study scenario. A smart city is conceptualized for developed countries but now this initiative got ample popularity in underdeveloped countries of the Asia Pacific and the Middle East. These Governments have been developing a unified standardized framework for converting metropolitan cities into smart cities. Major framework standards for analysis are designed by the British Standards Institute (BSI) smart city framework and the European smart cities framework.

BSI [14] has issued PAS 181:2014 [15] smart city framework guide publicly which serves as a guideline and compliance standard which recommends planning parameters for the development of smart cities. Main cardinals include empowering citizen's desires as a driving force behind all processes, integration of digital planning, fragile identification/anticipation and responses to upcoming challenges, and endorsing a change initiative for mutual delivery, integration, and innovation within organizational boundaries of the targeted city. BSI figures out the traditional city model, new integrated operating model and high-level structure. The first model is silo (non-inter connected) based which lacks mutual cohesion and cooperation, Operational model invests in smart data and inter-entity collaboration, High-level structure advocates a framework that depicts a comprehensive blueprint for smart city implementation tailored smart city circumstances.

BSI SCF emphasizes on the provision of a smart city roadmap with vital phases like planning, initiative, delivery, consolidation, and transformation. The high-level framework consists of four top-level modules such as guiding principles, key cross-city governance and delivery processes, benefits realization strategy, and critical success factor [16, 17].

Batty, et al. [10] presented the CISCO smart city framework which focuses on the use of technology, smart devices and automated systems for smart city initiative. It reiterates urban area's numerous challenges concerning population, economic growth, budget deficits solving via situational awareness based technological solutions using strengths of ICT. It aware users of technical modernization against possible eventualities and determines the archived level of technology. Its layers are city objectives, indicators, components, and content.

Smart city framework by Washburn, et al. [8] proposes a conceptual multitier framework (constituting six domains) that emphasized a holistic view of a smart city. It devises parameters like smart city services, interaction and integration with smart city infrastructures, smart city governance, case to case basis data collection of prevailing smart city initiatives and unit of analysis. This paper provides comparative analysis among cities of the US, Europe, and Asia spells out in maturity levels for smart city governance. Figure 2 shows the smart city architecture.

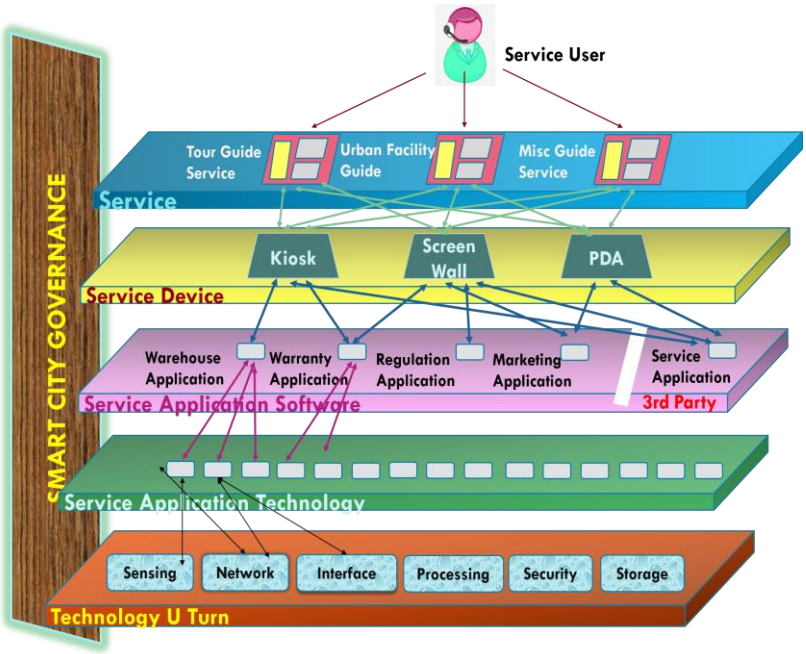

Figure 2. Smart City Architecture

Caragliu, et al. [9] developed a comprehensive ranking framework for medium-size European cities based on six characteristics, thirty-one sub divided factors and seventy-five indicators. This study is based on two hypotheses concerning the smart city's sustainability and prospects. Despite adopting a ranking approach, it lacks a standardized blueprint for the initial phase of smart city initiative development and integration focusses on already in place initiatives mandatory factors. Framework composed of modules like the smart economy, environment, governance, mobility, and living.

Chourabi, et al. [18] presented an integrated framework for a pure smart city. The proposed comprehensive set of factors that are essential for identification of success factors (further divided into inner and outer factors) for smart city implementation like organization and management, technology, Governance, policy, and regulations. It defines association among different factors and their influence on Initiatives. Technology is considered as the main core element the same as is in the CISCO framework, on which the success and failure of the remaining factors centers [18].

IDC insight smart city maturity model [19] framework proposes an evaluation of major technical and non-technical areas focusing on capitalizing benefits of smart city implementation. It is composed of key characteristics like Ad Hoc, opportunistic, repeatable, managed and optimized levels. Figure 3 shows the present & short-term status of cities.

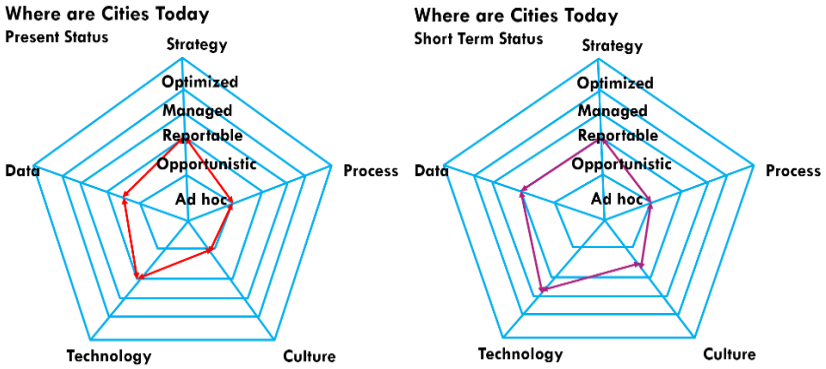

Figure 3. Present & Short-Term Status of Cities [14]

2.2. Cyber Security Mechanism for Smart Cities

This new concept can be described as a foundation framework provided by the National Security Council Secretariat of in 2016 [20]. It devised a generic architecture consists of 4 layers i.e. sensing, communicating, data and application, centrally controlled by a cyber-secure system. This architecture devised features and support which are open, scalable, and interoperable with each other with technology peculiarities. This framework is based on MoHUA's smart city cybersecurity guidelines based on salient like security governance, implementation, operation of security products/services, and security assurance. The framework applies security on all technologies based layers and allows each smart city to follow the same requirements as per centralized standards and complies with the futuristic regulatory landscape [21].

The security frameworks make systems more complex but it provides information assurance and security and such challenges are a bit acceptable if compared with data confidentiality issues. A security framework is devised which wholly based on the centralized processing and monitoring by maintaining information and data integrity, association and confidentiality over the secure mode of communications with end-to-end encryption of keys and data. Various cardinals of this framework include design and Governance addressing appointment of centralized security organization-assessments of business-driven risks establishment of a governing mechanism, advisory and incidence reporting of cyber threats, security operation addressing conducting-security operation as per security guidelines-design and operate an operational center with modernized capabilities. Figure 4 shows the smart cities' features, gaps, and recommendations from related work.

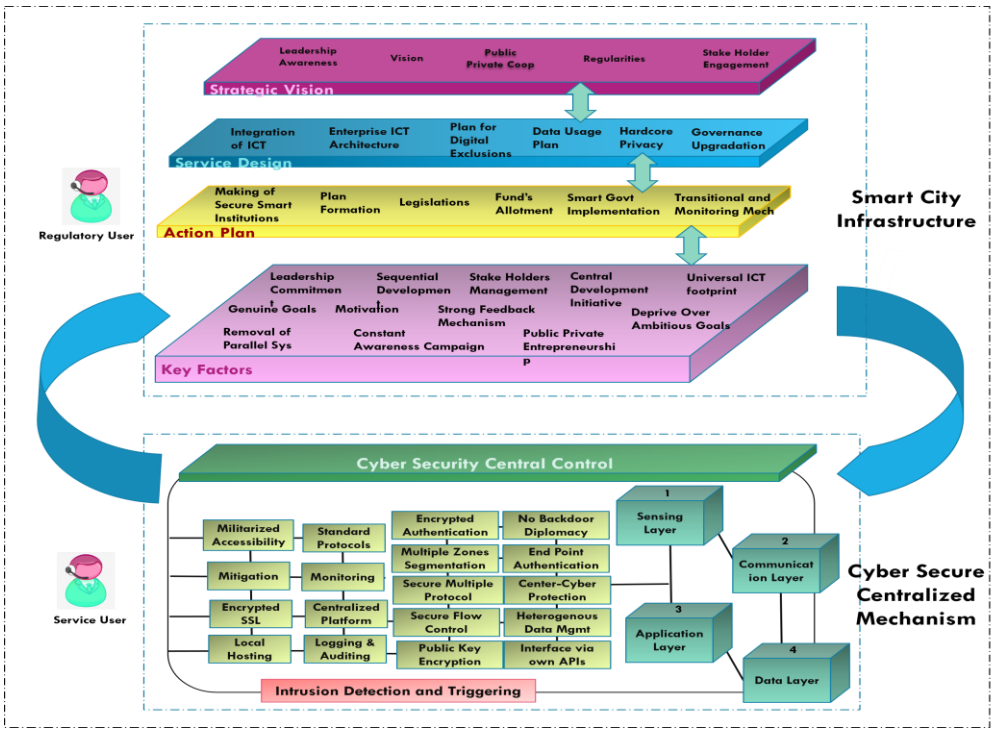

Figure 4. Cyber Secure-Smart City Framework

3. PROPOSED SMART CITY FRAMEWORK

The proposed framework is broadly distributed into two categories including smart city architecture and the cybersecurity central control which is illustrated as under:

3.1 Smart City Architecture

Frameworks are used for the creation of suitable and workable phenomena for the under-study scenario. A smart city is conceptualized for developed countries but now this initiative got ample popularity. These Governments have been developing a unified standardized framework for converting metropolitan cities into smart cities. The following are the main components are as follows:

Layer 1 - Strategic Vision. Strategic Vision is the top-level layer that consists of five components, which are leadership awareness, vision for cyber-secure smart city, public-private corporation, the regulatory framework for cyber-secure smart cities and engagement of stake holder's management.

a) **Leadership awareness:** The leaders should be aware of cyber-secure smart city governance benefits and aimed to implement it in different cities with true spirits. Moreover, to cope in the contemporary world realm, there is a dire need that leadership should follow their footsteps and adopts the possible fastest track to convert smart cities.
b) **Strategic Vision:** It is required to be visualized by Federal Government adaptable for provinces. In developed countries like the European Region and the US, this implementation is a bit different as cities initiative independently and processes are mostly bidirectional. In underdeveloped countries, control and implementation would be central and unidirectional.
c) **Regulatory Framework:** Creation of a regulatory framework for the design and development of cyber-secure - smart cities is the next step that would facilitate further progress.
d) **Collaboration:** Development of accountable public-private partnership without which this initiative will never be able to be materialized.
e) **Engagement:** Finally, the stake holder's engagement must be managed otherwise unfavorable forces would interfere and even get affected the supportive stake holder's community by adverse propaganda.

Layer 2 – Service Architecture. The integration of ICT and its governance is considered to be a core component in the cyber secure smart city and this aspect is common in discussed frameworks. An efficient ICT service architecture is mandatory for cyber-secure smart city deployment. Its components are Integration and Governance of ICT in respective echelons, enterprise city ICT architecture plan, data usage plan, hardcore privacy and security plan, outreach plan for digital exclusions and finally the strategy to up graduate governance towards the cyber secure smart city governance.

Layer 3 – Action Plan. Change is difficult with superlative degrees in our scenario so to drive change a comprehensive action plan should be chalked out which should not only implement change but would have a mechanism in place to sustain and maintain it also. It comprises different components naming as Legislation of Smart Governance, Formation of Smart Institutions, Development of Detailed Deployment Plans, Budget Allocations, Application and Employment of Smart Cities and finally Transformation and Monitoring Mechanism of a Secure Smart city.

Layer 4 – Key Success Factors. It shows the basic key success factors which should be considered for the successful application and employment of a cyber-secure smart city initiative. Those factors are namely Leadership Intent, Simple and Clear Goals, Phased Implementation, Cultural Transformation, Central Development Initiative, Citizen-Centric Design, Circumvention of Over Ambitious Goals, Strong Feedback Mechanism, Elimination of Parallel Systems, Continuous Awareness Campaign, Ubiquitous ICT Foot Print, and finally the Ownership by City Governments.

3.2. Cyber Security Central Control

Learning from the existing security mechanism being adopted for the smart cities framework; it is devised to adopt the same end to end data exchange and processing in an encrypted way via the secure all types of communicational channels adaptive to the standards being defined by the governing body centrally for all the smart cities under its control. In that case, the framework is being devised and the functionally and operational peculiarities are as under:

(1) Operational Peculiarities

a) Cybersecurity to be given the topmost priority for all the stakeholders involved during different operational phases of smart city development

b) Baseline security guidelines to be governed and implemented by the centralized governing body for implementation and configuration of all security-related modules.

c) The risk profile of different components of a smart city to be assessed considering Business-driven risks analysis to verify the selection of security products sequentially.

d) The mechanism for continual security assessment of smart city setup for identification and mitigation of security risks.

e) Development and grooming of cybersecurity awareness in the Smart City stakeholders so that they should be capable to maintain the hardcore and soft-core modules of cyber-secure smart city components with defined or authorized cybersecurity capabilities.

f) Cybersecurity budget allocation to be part of the overall smart city budget which should match the risk profile of smart city components to developing a delicate defense against any difficult proposition.

(2) Functional Peculiarities

a) All message exchange among different applications would be fully encrypted and authenticated and all communication from the exterior world would be done via predefined and exported APIs only,

b) The convergence of multiple platforms into the central platform for the ease of management in which adequate-authentication and role-based access control to be exercised,

c) In the multi-tenant architecture, there should be the provision of the data flow of normalized data only to authorized partitions of data with rules under adequate authenticity based on valid encryption mechanism,

d) Management of heterogeneous data administrated and managed via various devices under the shadow of numerous communication protocols,

e) Data layer should be capable to communicate with different types of sensors and devices whose data to be interoperable for processing, migration, and transportation among different supported applicable with the assurance of such via Data layer only,

f) The entire IT Infrastructure deployed as a cyber-secure - the smart city should follow standards like ISO-27001, ISO-22301, ISO-37120, BSI-PAS 182, for Wi-Fi access PEAP (Protected Extensible Authentication Protocol, 3GPP (3rd Generation Partnership Project) and related.

g) Generic APIs should be published and application should be based on standard protocols like JSON / XML / Html,

h) At network security level the information and data flow must be authenticated and secure via valid encryption and confidentially to be maintained at all the communication end ports and endpoints.

i) Plan for the Wireless broadband architecture should be Fiber Optical System based and should be interoperable and connective with other land and wireless communication devices.

j) Authentication system to be present at the nodal endpoints of all echelons of processing and communication systems capable of heterogeneous data management. To minimize the latency issues, standard network protocols to be used at different communication layers for data flow. All deployed applications should be indigenously hosted and developed.

k) Updating of all software and firmware's, all modules to be proficient in auditing and logging, elimination of backdoors and undocumented hard cored accounts to ensure compliance with vendor, peer to peer solution with full-service availability for which a service agreement should be materialized for a minimum period of 3 years since systems operations.

l) l) Appropriate teams to be in place for monitoring and mitigation of cyber incidents and information of such to be shared with Emergency Response Team and Federal Critical Information Protection Infrastructure Centre for recovery at any eventuality

4. SIMULATION AND EVALUATION

The proposed framework is analyzed in a virtual environment, for all the modules i.e. health, transport, finances the security framework. The overall total of 5 cities i.e. Islamabad/Rawalpindi, Karachi, Lahore, Peshawar, and Quetta is being conceptualized for the implementation of a smart city with cybersecurity aspects. Simulation parameters defined are for the measurement of QoS, Data throughput and reliability in any wireless (Wi-Fi) based network among different interconnected nodes of the smart city modules. Initially, almost 100-150 nodes are deployed in each smart city as per population size. Figure 5 shows the deployment of a virtual environment.

Figure 5. Deployment in Virtual Environment

Performance of proposed framework CSSC (Cyber secure smart city) and manual smart city channel selection based on the throughput and reliability is conducted. Channel is randomly chosen from the available pool of channels with 1/N probability and allocated to any process or transactional call without considering its QoS, whereas the proposed CSSC selects a secure channel with consideration of its QoS to reach the globally optimal solution. The cumulative distribution function plots min-max throughput of three types of channels as shown in Figure 6.

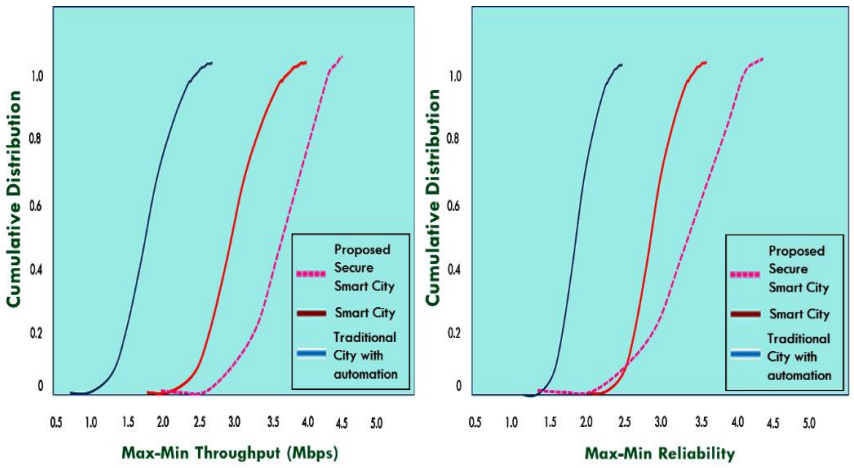

Figure 6. CF Analysis of Throughput and Reliability

Values are shown by adopting the Monte Carlo principle and average values over almost 600 iterations in a high network traffic mode. The graph's line plot shows gain almost 60-70 % as compared to legacy and smart city. CSSC shows the leading pattern and proves to be equally good for error-sensitive application transitions. From a reliability test, it shows CSSC provides more stable channels for secure traffic. In throughput analysis, it is visible that CF is stable initially for all three categories but with the rise in throughput, the cyber secure smart city achieves 1.0 level earliest. The smart city

follows a moderate trend being between two other approaches and adopts 2.0 to 3.5 Mbps throughput whereas CSSC possesses more throughput from 2.5 to 4.0 Mbps. In the case of testing reliability, CSSC adopts a trend of the traditional city but after the initial stage, it bypassing the Smart city curve and shows an upward trend in comparison with the other two successors.

For this research, both qualitative and quantitative research methodology has been adopted. In a qualitative aspects survey is conducted to analyze the response of different conceptualized cyber-secure smart cities to learn that how their local citizens use the smart application and platforms and what is their trend to get connected with local government facilities in the case of traditional smart city vs CSSC environment. Our analysis shows that digital applications and the proposed framework has remarkably increased the trend to adopt smart applications and has markedly increased the usage in numbers. Citizens in our survey felt more connected with the government after using the secure channel increased by almost 20%, results are shown in Figure 7.

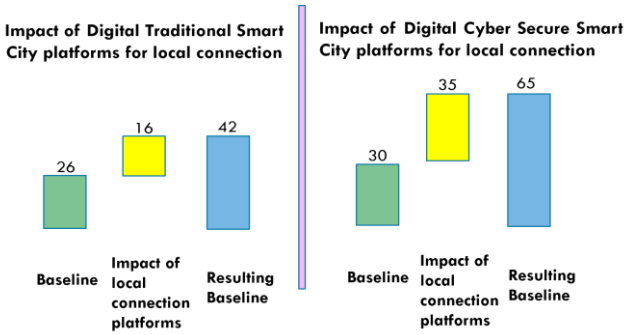

Figure 7. Comparison of Digital platforms

5. RECOMMENDATIONS

The cyber-secure technology-based governance may it be e-government or secure intelligent city governance is the future. From a few decades,' countries have worked diligently to implement smart city initiative with the blend of security. The following is recommended:

a) Governments intending up-gradation to capitalize on this initiative dividend and should start to secure smart city implementation on fast-paced programs.

b) Increase awareness in public about information/data privacy and security and its cost benefits.

c) Establishment of virtual layers in security mechanism for the creation of safety and disinfection of malware, Trojans and related virus threats.

d) Introduce automated machine aware, biometric and face recognition solutions by adopting liberal protection and detection and response algorithms to harden cybersecurity infrastructure.

e) The capital city is considered as a case study having well-acquainted citizens shows ample support for secure smart city initiative so indeed governing body needs to take advantage of favorable situations.

f) For smart cities, the initiative needs foreign investment along with the migration of highly skilled foreigner manpower. Such an initiative is a necessity for any state desirous to grow.

g) Brittan, South Korea, the US have put the systems in place and frameworks adopted there are only relevant to their specific conditions. Proposed framework and concepts are tailor-made for any scenario especially suitable for cities where the population is grave and security is a must.

h) The prevailing automated systems and initiatives (safe city projects, citizen's complaint system, transportation management, water management, electricity management, etc.) which are implemented in any modernized city of any country can be grouped under the cyber secure smart city framework to boost up this modernization program.

i) End to end multi-tier encryption is desired so that all transitions should be secure and use public-key encryption.

j) Continuous up-gradation of systems and conduct of training and testing activities to be conducted.

6. CONCLUSION

The study is a deliberate effort to explore such a research field which has scope for practical implementation and integration in the existing smart city implementation. The cyber-secure smart city ensures improved and reliable living for everyone, it promotes safety, protects the environment, creates better learning and job opportunities and ensures better deliverance of government services to the citizens. Paper comprehends cybersecurity concepts in smart city architecture, impacts on service delivery of systems, the synergy of these systems with smart city designs and works out the effective and practical framework for the Cyber Secure- Smart Cities. Adequate literature has been reviewed and analysis of the objectives and research queries has been done to establish, devise and demonstrate the proposed framework. The suggested framework is a small step taken towards cyber-secure smart governance and it is just a matter of time that we find cyber-secure smart cities instead of traditional smart cities embarrassing popularity and encouragement in new development projects.

References

[1] K. N. Qureshi, A. H. Abdullah, A. Mirza, R. W. J. I. J. o. E. Anwar, and C. Engineering, "Geographical forwarding methods in vehicular ad hoc networks," vol. 5, no. 6, 2015.

[2] K. N. Qureshi, A. H. Abdullah, and A. J. W. P. C. Altameem, "Road aware geographical routing protocol coupled with distance, direction and traffic density metrics for urban vehicular ad hoc networks," vol. 92, no. 3, pp. 1251-1270, 2017.

[3] K. N. Qureshi *et al.*, "A Dynamic Congestion Control Scheme for safety applications in vehicular ad hoc networks," vol. 72, pp. 774-788, 2018.

[4] S. Iqbal, A. H. Abdullah, K. N. J. C. Qureshi, and E. Engineering, "Channel quality and utilization metric for interference estimation in Wireless Mesh Networks," vol. 64, pp. 420-435, 2017.

[5] K. N. Qureshi, F. Bashir, and S. Iqbal, "Cloud Computing Model for Vehicular Ad hoc Networks," in *2018 IEEE 7th international Conference on Cloud Networking (CloudNet)*, 2018, pp. 1-3: IEEE.

[6] K. N. Qureshi, A. H. Abdullah, O. Kaiwartya, F. Ullah, S. Iqbal, and A. J. T. S. Altameem, "Weighted link quality and forward progress coupled with modified RTS/CTS for beaconless packet forwarding protocol (B-PFP) in VANETs," pp. 1-16, 2016.

[7] K. N. Qureshi and A. H. J. W. A. S. J. Abdullah, "Study of Efficient Topology Based Routing Protocols for Vehicular Ad-Hoc Network Technology," vol. 23, no. 5, pp. 656-663, 2013.

[8] D. Washburn, U. Sindhu, S. Balaouras, R. A. Dines, N. Hayes, and L. E. J. G. Nelson, "Helping CIOs understand “smart city” initiatives," vol. 17, no. 2, pp. 1-17, 2009.

[9] A. Caragliu, C. Del Bo, and P. J. J. o. u. t. Nijkamp, "Smart cities in Europe," vol. 18, no. 2, pp. 65-82, 2011.

[10] M. Batty *et al.*, "Smart cities of the future," vol. 214, no. 1, pp. 481-518, 2012.

[11] M.-P. J. J. o. I. Efthymiopoulos and Entrepreneurship, "Cyber-security in smart cities: the case of Dubai," vol. 5, no. 1, p. 11, 2016.

[12] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. J. F. G. C. S. Gupta, "Secure integration of IoT and cloud computing," vol. 78, pp. 964-975, 2018.

[13] M. Cavada, D. Hunt, and C. Rogers, "Smart cities: Contradicting definitions and unclear measures," in *World Sustainability Forum*, 2014, pp. 1-12.

[14] E. Theodoridis, G. Mylonas, and I. Chatzigiannakis, "Developing an iot smart city framework," in *IISA 2013*, 2013, pp. 1-6: IEEE.

[15] G. Falconer and S. J. C. I. B. S. G. Mitchell, "Smart city framework," vol. 12, no. 9, pp. 2-10, 2012.

[16] J.-H. Lee, M. G. J. R. P. Hancock, Yonsei University, and S. University, "Toward a framework for smart cities: A comparison of Seoul, San Francisco and Amsterdam," 2012.

[17] R. Giffinger, "European Smart Cities: the need for a place related Understanding," in *conference Creating Smart Cities, Edinburgh Napier University, June*, 2011.

[18] H. Chourabi *et al.*, "Understanding smart cities: An integrative framework," in *2012 45th Hawaii international conference on system sciences*, 2012, pp. 2289-2297: IEEE.

[19] R. J. I. G. I. Clarke, "Business Strategy: IDC Government Insights' Smart City Maturity Model—Assessment and Action on the Path to Maturity," 2013.

[20] S. J. I. P. Musa, "Smart cities-a road map for development," vol. 37, no. 2, pp. 19-23, 2018.

[21] E. Ferro, B. Caroleo, M. Leo, M. Osella, and E. Pautasso, "The role of ICT in smart cities governance," in *Proceedings of 13th international conference for E-democracy and open government. Donau-Universität Krems*, 2013, pp. 133-145.