frontiers in Computer Science

REVIEW
published: 13 October 2021
doi: 10.3389/fcomp.2021.736874

Cybersecurity Policy Framework in Saudi Arabia: Literature Review

Nawaf Alhalafi and Prakash Veeraraghavan**

Department of Computer Science and Information Technology, La Trobe University, Melbourne, VIC, Australia

Saudi Arabia has a goal of ensuring that it has at least two cities among the top 100 smart cities of the future. However, increasing connectivity and incorporation of smart solutions in cities still raises concerns over cyber security with threats arising daily including denial of services and phishing as some of the most significant. Saudi Arabia, therefore, needs a cybersecurity policy framework that will ensure effective protection for all stakeholders in the smart city from these cyber threats. User acceptance is foremost important in any new technology, including smart-cities. Due to ongoing cyber threats and in the absence of an efficient cyber policies, Saudi end-user community is not keen to accept newer technologies where their interaction with online medium is required. The proliferation of smart cities globally affords the opportunity to analyze and compare the efforts made in Saudi Arabia with other nations like the USA, India and Singapore which is the premier smart city model in the globe currently. This review looks at the similarities and differences between KSA's cyber security policy framework with these three nations. The review will note some of the defining characteristics and approaches to cyber security in the smart cities of USA, India, and Singapore. After reviewing the current framework in Saudi Arabia, this paper will make suggestions such as updating Saudi's cybercrime legislation like in the US or formulating a master cyber security plan as seen in Singapore that will improve KSA's framework creating the best framework model for cyber security in its smart cities.

Keywords: Smart Cities, cyber-attacks, cyber threat awareness, cyber competencies, cybersecurity analytics, user acceptance, cyber response, cyber resilience

OPEN ACCESS

Edited by:
Víctor Gayoso Martínez, Consejo Superior de Investigaciones Científicas (CSIC), Spain

Reviewed by:
Sukhkirandeep Kaur, Lovely Professional University, India
Andrey Chechulin, St. Petersburg Institute for Informatics and Automation (RAS), Russia

****Correspondence:***
Nawaf Alhalafi
17814379@students.latrobe.edu.au
Prakash Veeraraghavan
P.Veera@latrobe.edu.au

Specialty section:
This article was submitted to Computer Security, a section of the journal Frontiers in Computer Science

Received: *06 July 2021*
Accepted: *17 September 2021*
Published: *13 October 2021*

Citation:
Alhalafi N and Veeraraghavan P (2021) Cybersecurity Policy Framework in Saudi Arabia: Literature Review. Front. Comput. Sci. 3:736874. doi: 10.3389/fcomp.2021.736874

INTRODUCTION

The concept of smart-cities is not new. As soon as human civilization started, humans started planning to improve their lifestyles. With the rapid growth in information and communication technology (ICT) and the technology being accessible to more than 95% of the population, the civilization started using ICT for improving their lifestyle.

According to Twi-Global (Twi-Global, 2021), smart-cities effectively exploit the use of ICT to improve urban operational efficiency, immediate availability of information to the public and provide a better quality of government services and citizenship welfare. Synonymously, IBM defines smart-cities as follows (Twi-Global, 2021): "One that makes optimal use of all the interconnected information available today to better understand and control its operations and optimize the use of limited resources".

Every smart-city initiative around the world got one or more of the following visions: Effective use of the existing infrastructure and the technology; monitor environmental issues in providing greener technologies; congestion and pollution-free (This initiative is not only for good quality of life but also connected with pollution-related to carbon monoxide emission). Progressive and carefully planned

urban development is another critical vision. In the recent past, the world had witnessed mushrooming growth in unsustainable urban development. They lack public infrastructure, increase congestion, lack transportation, and does not use greener technologies. Thus, it made living uncomfortable, increasing stress and mental issues.

It is more desirable to live with a decentralized infrastructure in a smarter environment, where people can live and work within a shorter radius. Due to rapid urban expansion, the vast majority of people need to travel several hundred kilometres every day for their work or study. This resulted in severe mental stress, anxiety, and increased pollution. These factors have considerably reduced one's quality of life.

Even though smart-cities tried to address several challenges faced by urban living, there is no short of challenges in implementing them. Some of the crucial challenges are technical, socio-economic, and user acceptance.

With advances in ICT research and, technical challenges are diminishing day by day. Also, to note that technical challenges are not related to a particular city or a country. Since the technological outcomes are widely accessible to everyone, their challenges are homogeneous across every smart city initiative. Numerous survey and technical articles are addressing technological challenges in smart-city initiatives. Thus, in this work, we did not address any technological challenges. The economic challenges pose by smart-city initiatives in very important. Economic challenges can be addressed by establishing a more vital collaboration between public and private sector initiatives. We address this challenge in our next article.

User acceptance is critical for the success of any technology. The government must allow widespread participation from their citizens. There is also a need for private and public sector industries to align with citizens so that everyone can contribute to the success of the technology.

Social and cultural challenges differ from country to country. Even within a country, it differs between different regions. The same is true for smart-city initiatives. Smart cities were successfully deployed in the USA, Singapore, India, Japan, Canada, and Austria. However, a similar blueprint may not be used in Saudi Arabia for creating smart cities. The Saudi government must understand the social and cultural challenges that are unique to its citizens. This forms a strong motivation for this study. The outcome of this study will be followed through by establishing a series of a detailed policy framework for the Saudi government in successfully implementing the smart-city framework.

For this work, we considered USA, Singapore, and Indian smart-city initiatives. The reason for picking these countries is due to their cultural diversities. The motivation behind this survey is to establish the dissimilarities between various smart-city initiatives. Thus, unwrapping the potential cultural challenges and user acceptance issues in deploying smarter-cites.

Smart city Initiative in Saudi Arabia

The concept of smart cities is gaining immense popularity from across the globe as more nations seek to provide citizens with safe, modern, and convenient living spaces (Pandey et al., 2019). Smart cities utilize information technology and data networks to make better decisions and control aspects of the city like traffic management to improve the quality of life for its citizens. Smart cities are common in developed nations across the globe as information technology is incorporated into the management of cities. Saudi Arabia is one such nation with ambitions of having smart cities within its borders to carter for its growing population in major urban centers. According to the Kingdom's Vision 2030 manifesto, the goal is to have at least 10 smart cities in the Kingdom. The goal was to have at least five operational ones by 2020 with the following cities targeted: Riyadh, Makkah, Al-Ahsa, Jeddah, and Al-Madinah (Vitunskaite, He, Brandstetter and Janicke, 2019). The implementation of the smart city initiative is well underway in the country. However, there are concerns over an increase in cyber security risks as a result of proliferation of these smart cities. The purpose of this literature review is to compare Saudi Arabia's current cyber-security policy framework with that of other smart cities seen in the USA, Singapore, and India. Areas of relative weakness can be noted and possible recommendations made to improve the framework to align with the best practices in these other nations.

Smart city initiatives across the globe are on the rise as more governments seek to harness the advantages associated with a more interconnected urban setting. Some of the benefits associated with smart cities include more efficient distribution of resources, seamless communication, and more efficient implementation of policies. Efficiency in the distribution of resources is brought about by better organization and infrastructure management that is a hallmark of smart cities. Incorporation of IoT, sensors, and other systems in the city makes it easier to communicate real-time information on different aspects of city life. Policies are enacted faster and are more responsive to the needs of residents in smart cities.

The smart city initiatives in Saudi Arabia are seen in some of its cities including Riyadh, Jeddah, and Makkah. The push for more smart cities in Saudi Arabia is in line with the Kingdom's Vision 2030 manifesto that calls for a greater embrace of technology. Implementing smart city initiatives like Smart transport in the cities have been faced with technical and social challenges. Some of the technical challenges facing smart cities in the Kingdom include slow adoption of the same and a limited technical expertise workforce. The social challenges of smart cities is slow adoption of smart solutions and concerns over privacy and security.

The Saudi Arabian authorities can learn how to improve the smart city environment in the Kingdom by comparing the same with other similar initiative across the globe. The Saudi Arabian environment has factors that favor the growth of smart cities including a large, educated, and wealthy population. The kingdom stands to benefit from looking at how nations like the United States of America, Singapore, and India have managed to create a safe environment for their smart cities and means of improving cyber-security. The American environment is more liberal with a population that is quick in adopting new technology. Singapore has created an ideal environment to create a model smart city that serves its

residents (Von Richthofen et al., 2019). India has a large population that is open to enjoying the benefits associated with smart cities. This literature review will compare the cyber security measures in these nations with those seen in Saudi Arabia.

Current Cyber Security Models in Smart Cities: USA, Singapore and India

The concept of smart cities has quickly evolved from technology buzzwords to a practical goal for most nations around the globe. A smart city is one that puts technology and data to work together to improve decision making as well as improving the quality of life of its residents. A smart city is one that is based on a framework composed of information communication technology that promotes sustainable development practices. Smart cities are the future of urban living with the capacity to increase the efficiency of service delivery and improve the quality of life of individuals. According to Pandey et al. (2019), the typical smart city relies on digital technology, design thinking, and data to enhance the quality of services offered to residents. The proliferation of internet-enabled devices and technological advancements such as the Internet of Things (IoT) have increased the hyper-connectivity of people and systems.

Three layers work together to form a smart city. One of the layers is the presence of technology used in the collection of real-time data. The technology base in a smart city includes the presence of a critical mass of sensors and smartphones connected to a larger high-speed communication network. The second layer of what makes a city smart is the specific applications that transform data. Programs are needed to transform the raw data into meaningful actions, alerts, and insight. The final part of a smart city is the use of the information by the public, cities, and businesses. A city is considered smart if it can utilize its acquired and processed data into measurable actions that improves the life of its residents. Cities can significantly improve energy distribution and air quality, streamline waste management, reduce traffic, and improve security with the use of IoT on a smart city framework.

However, the reliance on interconnected systems in smart cities exposes them to cyber risks that could potentially have a negative impact on the function of the city (Alibasic et al., 2017). Cyber security, therefore, is a critical consideration in ensuring that the concept of smart cities is realized. The complex system of services, public and private organizations, people, workflows, infrastructure, and devices that constantly communicate with each other need to be secured to ensure prosperity for the people living within the city. The underlying infrastructure of the technology of smart cities can be divided into three components. The first step entails developing the edge comprising various devices, including IoT gadgets, actuators, smartphones, and sensors (Habibzadeh et al., 2019). The second critical component forms the central technology platform necessary to support and utilized the information obtained by the edge. Additionally, a communication channel is installed to support two-way exchanging of data between the smart city ecosystem and the edge (Habibzadeh et al., 2019). Cyber security threats can arise and compromise any one of these three components and disrupt the massive amount of data exchanges and integration taking place (Alibasic et al., 2017). Smart cities, therefore, need a cyber-security model that will protect their integrity and guide the response to potential attacks and threats.

The decision to have more smart cities in Saudi Arabia also has an impact on the culture of the people in the nation. Saudi Arabia, as expressed in its Vision 2030, has adopted a technology-friendly culture that is open to embracing smart solutions in the daily lives of citizens. More people in the kingdom are willing to embrace technological solutions in service access and delivery. The nation's culture is marked by a high level of acceptance and use of technology, although it is slightly less than the United States. This culture is expected to increase as more smart cities come up in the kingdom. The introduction of smart cities in Saudi Arabia is expected to have a positive impact on the culture of technology use.

This literature review will look at cyber security models in smart cities in the USA, Singapore and India and compare them with what is available in the Kingdom of Saudi Arabia. Moreover, the review will look at components from these other nations that could be incorporated in Saudi to improve its current protocol as well as those that cannot be transferred to the Gulf nation due to its unique nature.

USA *vs*. Saudi Arabia

Smart City Projects in the US

The United States has several cities that have integrated the use of data and technology to offer smart services to its inhabitants. Major cities across the country have incorporated the use of smart devices in their infrastructure to improve service delivery. A city like Dallas in Texas, for example, uses a smart water monitoring system to keep track of how water is used in the city and detect leaks. Texas, being an arid area, has to monitor the use of its scarce water resources. Dallas, in its attempt to be a smart city, hopes to leverage data on water use to better regulate its use and reduce waste in the city. The smart water system also detects leaks in real time ensuring prompt intervention and reduction of losses that would normally amount to thousands of gallons annually. The city of Chicago has an "Array of Things" project that has seen the smart use of data to improve service delivery (OCIA, 2015). The streetlights in the city automatically dim during the day and depending on the amount of sun outside, security cameras monitor activities, and water sensors look out for flooding along the riverbanks. The use of smart solutions in Chicago has improved security, reduced energy waste, and has helped the city avert flooding.

Many other cities in the United States have also followed the same path and qualify to be termed as smart cities with the incorporation of data, design thinking, and digital technologies to improve the service delivered to residents. Some well-known cities in the United States include Austin, Seattle, Charlotte, Boston, Washington DC, and New York. These major cities are actively incorporating smart solutions in various aspects of their infrastructure to ensure better service delivery. As American cities continue to incorporate smart solutions, the challenge of

cyber security threats continues to increase (Elmaghraby & Losavio 2015). These smart cities require protection from these threats to ensure their overall success and minimize threats such as distributed denial of services, phishing attacks, and Malware.

Potential Threats

The smart cities in the United States have experienced incidences of cyber insecurity. Dallas, for example, experienced an incidence where the Texas Health and Human Services Commission (HHSC) inadvertedly shared sensitive data of 6,617 patients (Kurtz, 2020). The breach came during a switch to a new server which happened to be public and unsecured. The combination of system and process blunders were investigated for HIPAA compliance and the body was fined $1.6 million (Kurtz, 2020). The intervention of the federal government showed the importance of having a centralized and coordinated approach to establishing and maintaining cyber security. Other incidences across America's smart cities that illustrated the ever present cyber security threats include the hacking of Omni Hotels and Resort in Dallas and the setting off of alarms by hackers in Chicago. All these events were addressed by strengthening the security features of databases as well as coordinated response from a federal or state body mandated to address cyber threats and security.

The United States relies on the Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA) to give infrastructural risk assessments on risks seen in the cyberspace. The OCIA provides a framework on risk recognition and mitigation in the growing smart cities in the nation. An OCIA (2015) report outlined how smart cities in the country can deal with growing threats to the cyber-physical space that exists. In addition to existing national laws against cybercrimes, the OCIA has suggested a three-tier approach to dealing with the threats to cyber cities in the nation. The first is to establish security in the changing seams that exists between legacy and new infrastructure as well as that between rural and urban centers. The seams between these spaces are shifting as systems become upgraded and networked. These changes provide opportunities for malicious activities and crimes. The OCIA recommends that smart cities monitor and protect against any attacks through this platform. The second recommendation given by the OCIA is to be more consistent with adoption of smart infrastructure. The body noted that critical infrastructure will develop at different paces and stages due to factors such as user preference, funding, and resources available (OCIA 2015). The concern of the organization is that the inconsistencies in the ecosystem will become a challenge and a major threat to the security of the smart city. The loopholes found in the overlap between the old and new systems create blind spots that make it easier for cybercrime to occur. The issue is inherent to many of the smart cities in the country as new technology is added to the legacy infrastructure. A consistent security policy is required in cities to ensure that it is successful. Finally, the organization calls for increased automation of processes in the smart cities. The proposal is to ensure that risks associated with human error are reduced.

Comparison With Saudi Arabia

Saudi Arabia has also enacted laws against cybercrimes and has dedicated institutions similar to OCIA in the United States. The Communications and Information Technology Commission (CITC) was established to oversee standardization in enacting regulations pertaining ICT (OCIA 2015). CITC has made efforts to oversee the current growth of the ICT sector in the nation. The organization provides permits to bandwidth companies, regulates the sector, and monitors the use of the internet within the borders of the nation. Saudi Arabia has passed ICT laws that criminalizes cyberattacks and any other malicious activities perpetrated online. The most comprehensive law in the nation is the Anti-Cyber Crime Law of 2007. The main difference between the legislation in Saudi Arabia and the US is that they are mainly based on Sharia laws. The Anti-Cyber Crime Law of 2007 prohibits the production of anything that is considered that is harmful to the public good, morals, and religious values. Other organizations in the country that deal with improving cyber security include the National Information Security Strategy (NISS) and the newly founded National Cyber Security Authority (NCA).

Singapore *vs*. Saudi Arabia

Smart City Project

Singapore is the ideal example of a smart city in the modern day. An IMD Smart City Index conducted in 2020 ranked Singapore as the smartest city out of a sample of 109 cities. The Asian city-state has made great strides in incorporating smart solutions in many of its services and infrastructure. Singapore is a global leader in smart health, mobility, and administrative solutions. Singapore has delivered in healthcare that is collaborative, people centric and encourages the use of innovative practices. The city has established a community-focused healthcare projects such as Health City Novena where residents can access quality medical care (Chia 2016). The health city in Singapore has several health facilities with the aim of providing innovative and quality healthcare. The facilities have embraced the use of technologies like remote monitoring devices and digital service platforms in delivering services to residents. Safety is also another key service in the city that has incorporated technology to ensure effective services are offered to residents. The Singapore police force has installed more than half a million surveillance cameras in the city and residents can access police-based services through online web-portals. Singapore is considered one of the safest cities in the world with the adoption of technological solutions.

Singapore is also a model city when it comes to smart mobility solutions. The authorities in Singapore have created effective public transport systems that are efficient, accessible, affordable, and ecologically sustainable (Šulyová & Vodák, 2020). A 2018 McKinsey report showed the Singapore has a best in-class transport system. Some of the smart solutions in transport currently include shared bicycle services, electric car pooling, and interconnected mass rapid transit (MRT) that has seen a significant increase in the use of public transport over the use of private cars. Finally, the city has incorporated smart solutions in delivering its administrative functions. The authorities have launched several projects like SingPass which is a national

digital identity portal. PayNow is an integrated e-payment service in the city for faster financial transactions. Moments of Life is another project that has seen the integration of all government services on one platform. The city state has become a model for harnessing information, technology, and digitization to improve the life of its residents.

Cyber Security Threats

As one of the leading smart cities in the world, Singapore is a prime target for malicious players in the cyber space. Overall, cybercrime in the Asian city accounted for 26.8% of all crimes within the city in the year 2019 (Koh, 2020). There were 9,430 cases reported in 2019 compared to 6,215 cases the previous year. The main cybercrime in the smart city of Singapore involves e-commerce scams targeting the vulnerable public (Koh, 2020). Other major cyber security threats detected in Singapore include phishing URLs, spoofing government agencies, and over 35 cases of ransomware reported against businesses in the city (Koh, 2020). The smart city has come up with robust laws and policies to guide cyber security protocols for citizens and businesses in the city as one means of combating these rising online threats.

According to Chia (2016), Singapore considers cyber security as one of the key enablers of its goal for a smart nation. The city's authority's advocated for creating a secure system that would protect the city from malicious attacks and distributed denial of services. In 2015, a 5-year National Cyber Security Masterplan 2018 was created. The document gave strategic advice and direction that would guide the city's efforts of ensuring cyber security is maintained as the city becomes more integrated with smart solutions (Von Richthofen et al., 2019). The guidelines apply to all stakeholders in the city and has the goal of creating a secure cyber-physical space that is vibrant and responsive to the needs of the population. Individuals are encouraged to follow these guidelines as Singapore's pool of critical smart infrastructure continues to grow.

Application to Saudi Arabia

A comparison between Singapore and Saudi Arabia shows some slight differences in their approach to securing their smart cities. The first is that Singapore relies on a master plan that is specifically focused on cyber security in the city while a similar plan does not exist in Saudi Arabia. The master plan in Singapore offers more comprehensive guidelines for businesses, governments, the private and the public sector to ensure that loopholes in the security of the smart city is contained. In Saudi Arabia, a set of fragmented laws and bodies are tasked with ensuring that cyber security is maintained.

India *vs*. Saudi Arabia

Smart City Projects in India

India has an ambitious target of creating 100 smart cities across the nation to improve service delivery and the quality of life of its citizens. The government noted that the urban population was increasing in size and importance as more people migrate into cities from the rural sides for education and employment opportunities. The aim of the country's leaders was to create more than 100 smart cities or municipalities across India where nearly 40% of the population will live and contribute close to 75% of the nation's GDP by 2030 (KPMG 2019). The cities are driven by smart solutions and advanced technologies that include smart mobility, e-governance, smart waste management, smart water management, smart healthcare, and smart energy management. The projects aim to reduce traffic congestion and improve mobility in the populous nation where traffic congestion is common in city streets. A smart waste management system and water management system improves the efficiency of trash collection and proper management of limited water supply respectively. Smart healthcare aims to improve health service delivery in cities where access to quality healthcare remains a challenge. These smart solutions are powered by state-of-the-art technology that help collect data and they include sensor networks, ubiquitous Network Connectivity, Smart Cards, IoT-based devices among many others (KPMG 2019). Much like in Saudi Arabia and other smart cities across the globe, the increasing reliance on smart solutions also raises the risk of cyber security breaches.

Cyber Threats

Smart cities in India have faced several online threats that threaten to impede service delivery and compromise the privacy of residents. Recently, due to the coronavirus outbreak, the cyber security threats towards the smart cities have been on the rise (Bagchi, 2021). The attacks come in different forms and include sophisticated attacks on vital infrastructures, halting the industrial control systems, as well as increasing incidences of ransomware. There have also been incidences where sensor data is manipulated to cause panic (Staff Reporter, 2019). These threats have been on the rise in Indian smart cities prompting a response from the authorities to form a standard approach to cyber security threats in the country.

How India Tackles the Cyber Threats.

India recognized the importance of setting up a cyber-security framework that would guide the establishment of smart cities and deter attacks (Vasileva et al., 2018). The Indian authorities addressed the cyber security needs of its smart cities by establishing a minimum baseline security standard, ensuring that there is security, privacy and trust in the ecosystem, and driving cyber security as a key component of all smart cities (Balaji 2017). Indian smart cities have adopted the use of both international safety standards as well as developing a local security model for cyber security known as "Office Memorandum". The Global City Teams Challenge Program outlines crucial international standards established and implemented by the National Institute of Standards and Technology (NIST) (Balaji 2017). The program saw the establishment of standards that can be applied globally to ensure cyber security is maintained in smart cities. NIST also produced an international working group that works on IOT-Enabled Smart City Framework to ensure that there is a standard approach to ensuring the safety of the residents from cyber-attacks and identity theft. Other guiding standards include ISO 37100, ISO 37120, ISO 39001, and ISO/IEC 30182 among many

TABLE 1 | Smart city initiatives in the smart cities' projects.

Smart city initiatives	USA	India	Singapore	Saudi Arabia
Smart water monitoring system	✓	✗	✗	✗
Digital technologies for service delivery	✓	✓	✓	✓
Framework on risk recognition and mitigation	✓	✗	✗	✗
User preference and Resources available	✓	✗	✗	✗
Remote monitoring devices	✗	✗	✓	✗
Modern Public transport systems	✗	✓	✓	✓
An integrated e-payment service	✗	✗	✓	✗
A master plan	✗	✗	✓	✗
E-governance	✓	✓	✓	✓
Smart waste management	✗	✓	✗	✗
Smart healthcare	✗	✓	✗	✗
Special Purpose Vehicle (SPV)	✗	✓	✗	✗
Workforce availability in cyber security	✓	✓	✓	✗
User acceptance	✗	✗	✗	✗

TABLE 2 | User acceptance in different smart cities' projects.

Smart city initiative	USA	India	Singapore	Saudi Arabia
User acceptance	✗	✗	✗	✗

others that touch on different aspects of smart cities (KPMG 2019). These guidelines are important in supporting technological advancements.

In the local context of India, The National Security Council Secretariat created a cyber-security model framework known as Office Memorandum that will guide the installation and use of information technology in smart cities. The framework gives a comprehensive guideline for stakeholders in smart cities to follow so that cyber threats are reduced to a minimum. The Smart City Special Purpose Vehicle (SPV) was also established by the Ministry of Housing and Urban to facilitate planning, managing, implementing, as well as assessing smart cities in the nation (KPMG 2019). The SPV is in charge of ensuring the smart cities remain cyber secure.

Application to Saudi Arabia

Differences between India and Saudi Arabia in terms of cyber security in smart cities exist. In India, there is great emphasis placed on international standards in guiding its approach to cyber security compared to Saudi Arabia. The framework established in India is unique to the nation whereas such as a comprehensive cyber security framework is lacking in Saudi. Finally, the use of SPVs in managing and monitoring smart cities and their security is unique to the Indian setup with no such arrangement in place in Saudi Arabia.

Through our literature, we compared 13 different smart-city initiatives covered by USA, India, Singapore and Saudi Arabia. We summarize them in the following table. A "tick" signifies that their proposal addresses that as shown in **Table 1** feature. "cross" signifies that a specific feature is not addressed by their smart city initiative..

It is interesting to note that none of the initiatives from USA, Singapore, India or Saudi had addressed "user acceptance" as shown in **Table 2**. In countries like USA, Singapore, and India, due to different socio-economic background, it may be easy to convince users to accept new technologies. However, we strongly feel the opposite in Saudi. Also, in other countries, the relationship between private and public sector industries are proven. The R&D initiatives through public-private sector initiatives is also well demonstrated in the past. However, Saudi is at an infant stage. Thus, we foresee as a potential challenge in successfully establishing smart cities.

Current Saudi Arabia Framework and Issues

Lack of a Comprehensive Framework

Saudi Arabia currently lacks a comprehensive framework for addressing cyber security challenges affecting its smart cities. The study proposes a cyber-security framework with five main components. The first is a digital trust platform to manage connections and seamless communication between different nodes in the ecosystem. The second part of the framework is a cyber-threat intelligence and analysis forum where cyber threats are actively monitored to ensure that they are mitigated effectively. The third component of the framework is cyber competencies and awareness programs to raise interest in the field and attract more people into the workforce. The fourth component is privacy-by-design that aims to protect the privacy of residents in the smart cities through the use of privacy standards throughout the ecosystem. Finally, the proposed framework has a cyber-response and resilience standard that would ensure smart cities are ready to effectively respond to any future cyber-attacks.

High Costs and Personnel

The main issues with the proposed framework are the cost as well as personnel required to implement the same, challenges with adoption, and a limited workforce in the field of cyber security. The proposed framework for Saudi Arabia's smart cities is comprehensive and cover several aspects of cyber security that would present as a challenge. However, the proposals will be costly to implement for the government. The five components of Saudi's cyber security framework necessitate significant

investment by the authorities. Developing a single digital trust platform for a population as large as one in the smart cities requires capital investment in hiring a development and maintenance team (Vitunskaite, He, Brandstetter and Janicke, 2019). The cost of acquiring the technology as well as the personnel is expected to be high for the Saudi authorities. Raising the level of cyber competence in the population requires investment of resources in public education and other programs to increase awareness of cyber security threats. A large percentage of Saudi Arabia population lack the necessary computer competency required to support smart cities, thus, necessitating reliance on expatriates to assist in the management of various aspects of the project. The government has a task in encouraging its citizens to enroll in computer courses to gain requisite skills. Saudi Arabia lacks a large workforce in cyber security compared to nations such as the United States and India, with more awareness needed to raise local interest in the field. Furthermore, it is difficult to convince skilled cyber security personnel to work in the public sector. Many skilled workers in the field prefer working in the private sector where the pay is higher and with increased benefits. Income needs to be reviewed for these personnel so that a balance is struck that would ensure the public sector is competitive and attracts top talent.

Time-Consuming

Implementing the framework is also a time-consuming endeavor. The five steps require sufficient time to develop, implement, and monitor for effectiveness. The comprehensive framework will take several years to implement as the smart cities of Riyadh and Naom continue to grow. The time required to fully implement the framework will leave the smart cities vulnerable to online attacks. It is recommended that other security features be put in place as the framework is being developed.

Cultural Influence on Policies

Another challenge in the adoption of the framework is the cultural influence on policies. There is a high level of uncertainty avoidance culture in Saudi Arabia that makes it harder to adopt new frameworks and policies without intense scrutiny first. Uncertainty avoidance culture in the Gulf nation influences the rate at which people are likely to understand, accept and adopt new policies and frameworks concerning cyber security and other forms of technology. The success of the framework will also depend heavily on the experience of the first adopters. Mainstream Saudi Arabians will need to first understand and observe the impact of the new framework before fully accepting it.

Additions to Saudi Model

Several components of frameworks outside of Saudi Arabia can be added to the proposed framework to make it more effective. From the United States model, Saudi Arabia can update its security laws to match the ever-evolving threats seen online. Saudi Arabia currently has the Anti-Cyber Crime Law of 2007 that is ambiguous in its interpretation and application. Creating comprehensive laws against cybercrimes as seen in the United States will improve the nation's response to cyber security in its smart cities. Saudi Arabia can also add a master plan that is specific for smart city cyber security as seen in Singapore. The Singapore smart city model has been extremely successful because of early formulation and implementation of a cyber-security master plan that guides the use of technologies in the city. From the Indian model, Saudi Arabia can borrow the idea of using SPVs to better manage the security threats in its smart cities.

What Cannot Be Added

Unlike India, Saudi Arabia should not rely heavily on international standards to guide the implementation of the framework. The cyber security framework of Saudi's smart cities should be tailored for the local market to ensure it is effective. There is, however, no other idea from India, USA, or Singapore that should not be added to KSA's cyber security framework.

CONCLUSION

Saudi Arabia is not alone in facing the challenge of ensuring cyber security is maintained in its smart cities. A look at the cyber security frameworks in other nations like the USA, India, and Singapore hold valuable lessons for KSA. In the USA, cyber security in its various smart cities is ensured through legislations passed in Congress and the OCIA guidelines. In Singapore, a master plan on cyber security is the main guideline for ensuring cyber security while India has adopted the use of international and local frameworks as well as SPVs to manage smart cities. Saudi Arabia can imitate some of these processes to make its cyber security framework more effective.

AUTHOR CONTRIBUTIONS

NA and PV helped write and complete this paper.

REFERENCES

Alibasic, A., Junaibi, R., Aung, Z., and Woon, W. (2017). Cybersecurity for Smart Cities: A Brief Review. *Comp. Sci.*, 1. doi:10.1007/978-3-319-50947-1_3

Bagchi, S. (2021). *Why Smart Cities are Sitting Ducks for Cyber Criminals*. [online] CXOToday.com. Available at: https://www.cxotoday.com/security/why-smart-cities-are-sitting-ducks-for-cyber-criminals/ (Accessed June 2, 2021).

Balaji, A. P. (2017). 'The Journey in Making 'Smart Cities' Smarter with Solar Energy. *Int. J. New Tech. Res. (Ijntr)* 1, 21, 2017 . Available from [1 May 2021]. doi:10.1007/978-3-030-15145-4_63-1

Chia, E. S. (2016). *Singapore's smart nation program — Enablers and challenges.' 2016 11th System of Systems Engineering Conference (SoSE)*. Singapore: Eng. Seng Chia. Available from[1 May 2021]. doi:10.1109/sysose.2016.7542892'

Elmaghraby, A. S., and Losavio, M. M. (2015). Cyber Security challenges in Smart cities: Safety, Security and privacy. *J. Adv. Res.* 5, 491–497. doi:10.1016/j.jare.2014.02.006

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., and Soyata, T. (2019). A Survey on cybersecurity, data privacy, and policy issues in cyber-physical System deployments in Smart cities. *Sust. Cities Soc.* 5. doi:10.1016/j.scs.2019.101660

Koh, D. (2020). *Singapore Cyber Landscape*. Singapore: Cyber Security Agency of Singapore. [online] 2(1). Available at: https://portswigger.net/daily-swig/singapore (Accessed June 2, 2021).

KPMG (2019). Cybersecurity in Smart cities. Available from https://assets.kpmg/content/dam/kpmg/in/pdf/2019/02/Cybersecurity-in-smart-cities.PDF May 1, 2021.

Kurtz, S. (2020). *Top Dallas Cybersecurity Breaches and How They Could Have Been Avoided*. [online] Dallas Texas - Total IT. Available at: https://totalit.com/top-dallas-cybersecurity-breaches/ (Accessed June 2, 2021).

OCIA (2015). *Office of Cyber and Infrastructure Analysis*. Washington, DC: US Department of Homeland Security. Available from https://us-cert.cisa.gov/sites/default/files/documents/OCIA-TheFuture of Smart Cities-Cyber-Physical Infrastructure Risk.pdf May 1, 2021.

Pandey, P., Golden, D., Peasely, S., and Kelkar, M. (2019).Making Smart cities cybersecure: Ways to address distinct risks in an increasingly connected urban future. Deloitte. Available from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf May 1, 2021.

Staff Reporter (2019). *Smart City and related Cyber Security Concerns In India - dynamicCISO*. [online] dynamicCISO. Available at: https://dynamicciso.com/smart-city-and-related-cyber-security-concerns-in-india/ (Accessed June 2, 2021).

Šulyová, D., and Vodák, J. (2020). The impact of cultural aspects on building the Smart city approach: Managing diversity in Europe (London), North America (New York) and Asia (Singapore). *Sustainability* 12, 22. doi:10.3390/su12229463

Twi-Global (2021). What is a Smart city. Available from https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city Sep 08, 21

Vasileva, R., Rodrigues, L., Hughes, N., Greenhalgh, C., Goulden, M., and Tennison, J. (2018). What Smart campuses can teach us about Smart cities: User experiences and open data. *Information* 9, 10, 2018 . Available from. doi:10.3390/info9100251

Vitunskaite, M., He, Y., Brandstetter, T., and Janicke, H. (2019). Smart cities and cyber Security: Are we there yet?A comparative Study on the role of Standards, third party risk management and Security ownership. *Comput. Security* 83, 313–331. doi:10.1016/j.cose.2019.02.009

Von Richthofen, A., Tomarchio, L., and Costa, A. (2019). Identifying communities within the Smart-cultural city of Singapore: A network analysis approach. *Smart Cities* 2 (No. 1), 66–81. Available from. doi:10.3390/smartcities2010005

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.