IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework

Ishaq Azhar Mohammed

Sr. Data Scientist & Department of Information Technology

Dubai, UAE

Abstract- *The main aim of this paper is to analyze the security, privacy, and risks in intelligent smart cities in the context of smart cities engagement. One of Smart City Technologies' aims is to collect data to evaluate people's and activities' real-time awareness and to provide decision-makers with information on their effect. Using so-called "behavioral economics," authorities may launch programs that, ideally, will alter conduct for the general benefit. One example is predictive policing. Another includes speed monitoring devices to urge individuals to drive in residential areas more gently. But these sophisticated technologies, if utilized incorrectly, may lead to poor policy [1]. For designers, integration partners, and organizations engaged in the administration of these new organizations, the complex and interconnected structure of intelligent cities presents major political, technological, and socio-economic difficulties. A large body of literature concentrates on the security, privacy, and vulnerabilities in smart cities, emphasizing concerns related to information security and difficulties in the administration and confidentiality of the data for secure networks [1]. This research analyzes several of these issues, gives a useful summary of the relevant important literature, and provides a framework for intelligent city interactions. The report involves numerous key topics within smart cities analysis: data protection and safety for mobile technologies and networks; intelligent infrastructure needs, power grids, medical services, institutional arrangements, methodologies and data protection guidelines, operations and maintenance threats to smart cities, the use and implementation of smart service provision for residents, use of blockchains and the use of social networking sites [2]. This thorough analysis gives a helpful picture of many of the major problems and provides important guidance for future research. The findings of this study will offer researchers and professionals an instructive theoretical framework and point of reference.*

Keywords: *Access control, risk-based access control, security risk, risk factors, risk estimation techniques*

I. INTRODUCTION

Computing and telecommunications technological advances have dramatically changed the globe. The development of the Internet of Things and cloud computing was utilized in particular for improving the quality of services in cities. The growth of microprocessors, internet technologies, and strong data networks have made information technology an essential tool for both private and public stakeholders [2]. Technological advances, like cloud computing systems, digital devices, networks, sensor systems, and artificial intelligence capabilities are used by Smart City architects to allow the many elements of smart cities to coordinate and communicate with the routing protocol. The intrinsic complexity and innovative approaches to citizen engagement needed to alter the current infrastructure highlight major difficulties for governments and regional authorities in political, regulatory, and technological fields. Smart cities have several difficulties, including data processing and administration. A smart city's security and privacy are impacted by the connecting of data from existing municipal databases with new technologies and sensors [2,3]. The risks resulting from the security of information, privacy, and cyber-related variables in which unauthorized access to information may have unwanted effects emphasize the severity of providing answers to questions early in the creation and development phase of smart cities.

To illustrate, the increasing significance of cities' economic and social elements in strategic plans has resulted in the adoption of new technologies [3]. The idea of smart cities arises from the combination of information, connectivity, and sophisticated sensors to manage municipal assets. Sensor networks serve a vital role in collecting crucial information on the urban environment in particular. It is feasible to send

real-time information using camera processors and data networks [4]. The increase in the population is the biggest contributor to the demand for intelligent infrastructures. Intelligent cities enhance the sustainability and effectiveness of many urban dynamics, like health, transportation, housing, and electricity [4,5]. A deeper study shows that the use of intelligent technology is successful in urban areas and is subsequently expanded to other regions before a nationwide and even international network is formed. Due to the necessary connection between sensor nodes [5,6], the idea of the Internet of Things (IoT) has become fundamental to the conceptualization and development of Smart Cities. Although it is a disputed concept, an intelligent city refers to the optimal utilization of resources by using real-time technology that automates certain tasks [7]. Indeed, sensor technology is crucial for cities since they have quintessence and functionality. It is thus essential to investigate methods in which municipal authorities may apply these advances in the development of smart urban areas, because of the inconsistency of the power of sensor technologies.

The fundamental organizational framework of the intelligent city includes advances in communications, data analytics, Internet of Things (IoT) development, and a range of physical infrastructures for smart operations management. The government has a crucial role to play in the development of any smart city, from the planning stage through to the implementation and operation of initiatives. Smart cities are therefore an all-encompassing city development paradigm that improves control and efficiency while also promoting inclusiveness via the use of contemporary technology to create improved functioning and sustainable development for all residents [9]. A limited view is that the smart city can only be thought about technology and connectivity. In practice and theory, the smart city uses technology to make more informed choices for the government, the public, and commercial organizations, and increase the productivity and sustainable growth of society. Intelligent city technology has been acknowledged to play an essential part in attaining sustainable development in modern times. To that aim, many cities across the world have used intelligent technologies to optimize urban infrastructure and services to enhance socio-economic conditions, healthier environment, and increase their competitiveness and attractiveness globally. Researchers seem to have failed to analyze meaningfully the important risks to data security and the complexity that surround privacy in intelligent cities [9]. This study attempts to fill this literature gap by analyzing in-depth the numerous problems and the major complexity in smart cities related to privacy, safety, and risk issues. The main aim of this paper is to analyze the security, privacy, and risks in intelligent smart cities in the context of smart cities engagement. One of Smart City Technologies' aims is to collect data to evaluate people's and activities' real-time awareness and to provide decision-makers with information on their effect. Using so-called "behavioral economics," authorities may launch programs that, ideally, will alter conduct for the general benefit. One example is predictive policing. Another includes speed monitoring devices to urge individuals to drive in residential areas more gently. But these sophisticated technologies, if utilized incorrectly, may lead to poor policy [11]. For designers, integration partners, and organizations engaged in the administration of these new organizations, the complex and interconnected structure of intelligent cities presents major political, technological, and socio-economic difficulties.

II. PROBLEM STATEMENT

The main problem that this paper will try to solve is to review the security, privacy, and risks in smart cities. With urban centers increasing their dependence on automated sensors and algorithms, they raise the danger of infringement on data security, vulnerability to privacy invasions, and software dependability issues. A large body of publications concentrates on the security, privacy, and vulnerabilities in smart cities, emphasizing concerns related to information security and difficulties in the administration and confidentiality of the data for secure networks [11]. This research analyzes several of these issues, gives a useful summary of the relevant important literature, and provides a framework for intelligent city interactions. The report involves numerous key topics within smart cities analysis: data protection and safety for mobile technologies and networks; intelligent infrastructure needs, power grids, medical services, institutional arrangements, methodologies and data protection guidelines, operations and maintenance threats to smart cities, the use and implementation of smart service provision for residents, use of blockchains and the use of social networking sites [12]. This thorough analysis gives a helpful picture of many of the major problems and provides important guidance for future research. The findings of this study will offer researchers and professionals an instructive theoretical framework and point of reference.

III. LITERATURE REVIEW

A. Smart City Technologies

Intelligent city technology depends heavily on wireless IP networks that are increasingly susceptible to hackers. These networks link up to a better performance, such as the reduction of power waste by electricity networks, traffic management systems intended to decrease congestion throughout the city's road and road networks, and smart water systems. The US Homeland Security Department published a report examining the cybersecurity threats of intelligent cities. The future of intelligent cities: cyber-physical infrastructure Risk split the topic into three subjects covering security issues for intelligent infrastructure. First of all, the "seams" between rural and urban areas and heritage and modern components of the infrastructure are shifting or vanishing. As a consequence, transport, electricity, and water networks are becoming more porous and accessible from a distance [12]. While technology improves connection and accelerates data flows, it also extends the boundaries that cities have to ensure.

Secondly, the study highlighted worries about "incoherent adoption" of intelligent technologies because of limited resources or consumer readiness, such as independent cars, to utilize this technology. An uneven shift to these technologies increases safety risks, such as 'blind spots,' in which old and new technologies have not blended to full and can notify concerns. There is also the financial problem for utilities that have to pay for an intelligent grid solution while retaining a manual backup system in the event of a failure. Intelligent city-systems minimize human contact to enhance computer efficiency. The number of security points only increases as cities move to data-driven and sensor-based solutions, while manual override mechanisms are decreased and human capabilities are atrophied. Another concern is that smart systems are too dependent on operating key infrastructural parts or increasing the efficiency of municipal services. Anything could go wrong. Just consider the assumptions in HealthCare.gov that crashed when too many individuals signed in [12].

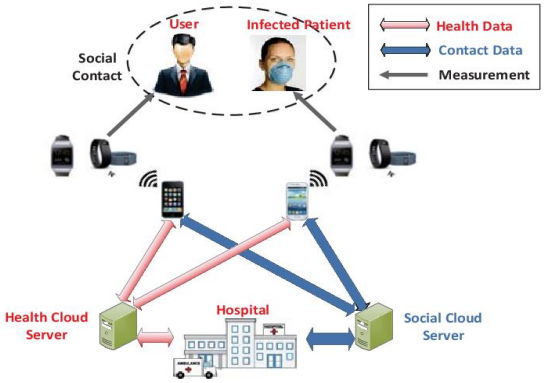

Fig i: Interaction of smart technologies in a smart city

B. Accessibility and Application of Smart Technology

In the development of smart cities, many cities, particularly in the north, continue to utilize the benefits of sensor technology. The ever more complicated integration of citizen involvement, IoT, and the various fields of intelligent town applications needs knowledge of the data produced for the realization of effective urban planning [12,13]. Smart urban planning, infrastructure management, and public engagement, for example, have distinct data-based needs. Each application thus adopts a different strategy for the creation of its intelligent network. For example, the smart city idea was created to tackle the security problem among its users. The growth of the IoT internet is a key intelligent network for Smart Cities development [13]. Crowdsensing needs the internet of people to offer Smart Cities security. Crowdsensing is used in particular to identify and regulate people in crowds or congested roadways. The crowd sensing system is a smart network that needs trustworthy data detected by the auction-based method. Non-technical ideas needed to make crowd-sensing data easier to available include users' rewards. Another aspect of the use of smart networks is the importance of residents' privacy in the smart city [13]. Privacy is a key component of security whose breach is a significant danger to the creation of efficient intelligent cities.

C. Challenges in Smart City

There are also difficulties to overcome for all the advantages provided by smart cities. These are government officials who enable broad public involvement. Private and governmental sectors need to connect themselves with citizens so that everyone may contribute positively to the community. Smart city initiatives must be transparent and accessible to residents via an open data site or mobile app [14]. This enables people to communicate with the data and do their activities, such as payment of accounts, efficient travel, and energy consumption assessment at home. All of this needs a robust and safe data collecting and storage mechanism to avoid hacking or abuse. Smart city data must also be anonymized to avoid privacy problems. The biggest issue undoubtedly is connectivity, which requires hundreds and perhaps millions of IoT devices to connect and operate together [14]. This will enable services to be linked together and continuous improvements to be made with increasing demand. Technology aside, intelligent cities also need to take care of social aspects that create an appealing and locally sensitive cultural fabric. This is especially essential for those cities which are built from the ground and which need to attract inhabitants.

D. Smart Cities Security

Smart cities provide lots of advantages to enhance the safety of the public, such as linked surveillance systems, smart roads, public safety monitoring. Smart cities need to be secured against cyber assaults, hacking, and data theft while also ensuring sure the provided data is correct. To control the security of intelligent cities, mechanisms like physical data valves, robust authentication management, and IT solutions need to be implemented [14]. Citizens must trust smart cities' safety and that implies that governments, private companies, software developers, device makers, energy suppliers, and network services managers must work together to provide integrated solutions with key safety goals. These fundamental safety goals may be divided as follows:

1. Data availability – Reliable access is needed in real-time to ensure that it fulfills its role of monitoring the different elements of the smart city infrastructure
2. Integrity - Data must also be accurate and not only easily accessible. This also includes protecting against external tampering.
3. Confidentiality - Sensitive information must be kept private and secure against unauthorized access. This may include the deployment of firewalls or data anonymization
4. Responsibility - System users must be responsible for their activities and interactions with sensitive data systems. User logs should document who accesses the information to provide responsibility should issues arise. Legislation in several countries such as the U.S. IoT Cybersecurity Improvement Act is already in place to assist in determining and establishing baseline safety standards for connected devices in smart cities.

D. Frameworks and Protocols to Improve Security and Privacy

Since intelligent cities confront a variety of security and privacy problems, several researchers suggested different frameworks, models, and algorithms to address these issues. This part of the literature focuses on encryption methods for smart city systems. Nothing about the data would be disclosed by the application of this technology during any data violation. Similarly, encryption is employed in the proposal of a system entitled Fully Data Protection and Revocable Broadcast Encryption on Identity (FPPRIB) [14]. The proposal aimed at protecting the privacy of data and the privacy of the recipient and the revoked user. Data may be securely secured and data can be accessed only by the authorized user. No data about the data content or the recipient identity can be obtained during the revocation procedure and the public is not aware of the recipient identity and the revoked user identity. These characteristics lead to smart city applications where the secrecy of identification is desired. SMARTIE is a user-focused integration platform for secure IoT applications. It safeguards the privacy of users while ensuring scalability and efficiency [14]. The suggested architecture effectively decentralizes IoT device access control depending on user privacy choices. SMARTIE aims to enable the integration of user-centered privacy and government inside a city, thus preserving the privacy of user data to finalize access to the network for the customer. The PrivacyZones Privacy Framework, which compels the service provider to disclose significant aspects of data gathered in its application, is another suggested framework. Two case studies services were used to effectively test the proposed framework. The use of AI in intelligent cities may enhance security and privacy [15].

Smart City Interaction Framework

The context provided in Fig.3 emphasizes and combines the many interdependencies between the many variables and problems highlighted in sustainable development. The model describes the effect of the main problems on the different operational activities of the smart city and contextualizes sustainability initiatives with important variables such as services and transportation. The model incorporates representations of the complexity associated with privacy, security, and risk in smart grids across all of its components [15]. These elements are essential to smart city operations that need efficient procedures and policies at all dimensions

of major infrastructure meaningful interactions. The main difficulties for clever cities such as confidence, operations, and transition, technical, and sustainability are highlighted and the emphasis is placed on smart city designers and integrators. The main issue of creating public trust is to extend the operational reach and to connect effectively with smart city services and infrastructure. No smart city system or interface can function unless all stakeholders trust it. Experiences of digital denominations and reluctance to connect may be evidence of a poor level of trust when people are concerned about security or risks to the integrity of personal data [16]. The selected smart city elements are based on literature research and the themes highlighted, namely: services, connectivity, protocols, legislation and regulation, wellness, quality of life, and governance. Each is a set of elements needed to operate successfully in the smart city. Substantial dependence on human elements and their interplay for the development of smart cities is emphasized by the major players, i.e. people, governments, and organizations. As cities have the smarter capacity, significant difficulties persist. Consequently, the development of intelligent cities and the difficulty for authorities is establishing confidence via data protection and security efforts, and the effect on people's lives and well-being is considerable. The operational risks in smart cities are diverse and rely on many elements of security strategy, learning, and the successful balancing of transparency and accurate measurements of intrusion and safety. These issues are continuing difficulties for future intelligent city projects 16].

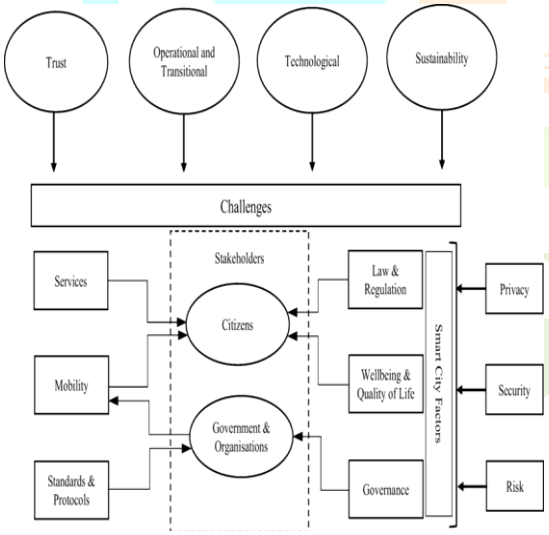

Fig ii: Smart cities security & privacy framework

IV. FUTURE OF RESEARCH

Smart cities and the Internet of Things (IoT) are perhaps the most important technological developments in the United States, and the way we live our lives has already been transformed. Some of the largest potential customers for these technologies are metropolitan areas and governments that are creatively trying to address long-standing issues. These emerging intelligent cities confront rising demand from their citizens and very little leadership from the federal and state authorities [17]. Nevada uses intelligent technology to improve the circulation of firearms in Las Vegas, Birmingham, Alabama, by employing a high-tech network to recognize shootings. As the preceding examples show, intelligent cities may enhance the health of the population. Nevertheless, there are issues about the deployment of intelligent city technologies, with special emphasis on privacy and security. Because of these complications, numerous proposals have been tabled by the US Congress has enacted bills to allow businesses and communities flexibility and assistance (through financing and coordination) to innovate while also putting down guards to alleviate possible negative externalities [18].

V. ECONOMIC BENEFITS

More technical needs for the US IT sector will be beneficial as security problems continue to grow. The number of devices linked to IoT is predicted to increase from 6.6 million in 2016 to 22.5 billion as costs for IoT devices, storage, and compute continue to decrease. This increased accessibility of IoT devices will boost the number of intelligent city projects and the quantity of cyber-physical data [18]. In the next 20 years, local governments are expected to spend up to $41 trillion on intelligent technologies to enhance their infrastructure, according to the Smart America Challenge. Many US towns already use different smart city technologies and optimize data from the cyber-physical environment to solve a broad range of issues and eventually make their cities more efficient and viable. The Smarter DC project focuses on helping to develop intelligent urban planning frameworks, interoperable norms, replication, scalable and sustainable models. The continued growth of the Internet economy in the United States is dependent on the proper management of online identification information. A biometric authentication system utilizes smart technologies. A number of these smart cities have purchased a few technological startups over the years to extend their service portfolio, and they are constantly upgrading their products and service portfolios [18]. The continued growth of the Internet economy in the United States is dependent on the proper management of online identification information [18]. As a result of the increased need for secure identification and access management services, the area will be able to strengthen its hold on the identity and access management market share in the future years.

VI. CONCLUSION

This paper discussed the various aspects of smart cities in terms of frameworks to address issues like privacy, risks, and security. The findings from this research demonstrate that creating smart connected systems in our urban areas brings significant advantages not only to better quality of life but also to guarantee sustainability and optimal use of resources for people across the globe. In today's cities, networks of interconnected technology are developing to produce actionable data on themselves and their people, sometimes instantaneously. Smart buildings routinely gather information on the air quality, temperature, noise, road and pedestrian traffic of urban centers, parking capabilities, distribution of government programs, emergencies, and crowd sentiment, among other data points, using omnipresent telecommunications technology to provide communication links to sensor networks and implement control equipment. These solutions rely on a united approach by the government, the business sector, and the people themselves. Smart cities may, however, utilize the right support and infrastructure to improve resident life and develop integrated live solutions for the increasing global urban population, like the Internet of Things.

REFERENCES

[1] L. Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective", SSRN Electronic Journal, 2016.

[2] A. AlDairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies", Procedia Computer Science, vol. 109, pp. 1086-1091, 2017.

[3] A. Elmaghraby and M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy", Journal of Advanced Research, vol. 5, no. 4, pp. 491-497, 2014.

[4] B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes", Sensors, vol. 18, no. 3, p. 817, 2018.

[5] S. Alromaihi, W. Elmedany and C. Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications", 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2018.

[6] J. Hubaux, S. Capkun and Jun Luo, "The security and privacy of smart vehicles", IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 49-55, 2004.

[7] A. Picon, "Opinions · Smart Cities, Privacy and the Pulverisation/Reconstruction of Individuals", European Data Protection Law Review, vol. 5, no. 2, pp. 154-155, 2019.

[8] K. Kimani, V. Oduol and K. Langat, "Cyber security challenges for IoT-based smart grid networks", International Journal of Critical Infrastructure Protection, vol. 25, pp. 36-49, 2019.

[9] S. Chatterjee, A. Kar and M. Gupta, "Critical Success Factors to Establish 5G Network in Smart Cities", Journal of Global Information Management, vol. 25, no. 2, pp. 15-37, 2017.

[10] L. Cagliero, T. Cerquitelli, S. Chiusano, P. Garino, M. Nardone, B. Pralio and L. Venturini, "Monitoring the citizens' perception on urban security in Smart City environments", 2015 31st IEEE International Conference on Data Engineering Workshops, 2015.

[11] S. Alter, "Making Sense of Smartness in the Context of Smart Devices and Smart Systems", Information Systems Frontiers, vol. 22, no. 2, pp. 381-393, 2019.

[12] E. Kenneally, "Intelligent Data Security and Privacy for Smart Cities", IEEE Internet of Things Magazine, vol. 2, no. 3, pp. 7-9, 2019.

[13] C. Shih, J. Chou, N. Reijers and T. Kuo, "Designing CPS/IoT applications for smart buildings and cities", IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 3-12, 2016.

[14] A. Sanjay, M. Vijarania and V. Jaglan, "Security Surveillance and Home Automation System using IoT", EAI Endorsed Transactions on Smart Cities, p. 165963, 2018.

[15] H. Khurana, M. Hadley, Ning Lu and D. Frincke, "Smart-grid security issues", IEEE Security & Privacy Magazine, vol. 8, no. 1, pp. 81-85, 2010.

[16] J. Lala and F. Schneider, "IT Monoculture Security Risks and Defenses", IEEE Security & Privacy Magazine, vol. 7, no. 1, pp. 12-13, 2009.

[17] M. Losavio, K. Chow, A. Koltay and J. James, "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security", Security and Privacy, vol. 1, no. 3, p. e23, 2018.

[18] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid", IEEE Security & Privacy Magazine, vol. 7, no. 3, pp. 75-77, 2009.

[19] D. Rosenblum, "What Anyone Can Know: The Privacy Risks of Social Networking Sites", IEEE Security & Privacy, vol. 5, no. 3, pp. 40-49, 2007.