British Journal of Research
ISSN: 2394-3718

Open Access Research Article

Smart Cities Security: Systematic Review

Halla Alharbi*

Department of Information and Computer Science, College of Computing and Mathematics, Dhahran 31261, Saudi Arabia

ABSTRACT

As cities become smart that are increasingly digitalized and interconnected, the need for robust cyber security measures in urban environments becomes more pressing. This systematic review aims to evaluate the current state of research on smart city cyber security, with a specific focus on the challenges and solutions related to protecting critical infrastructure, personal data, and public safety. The review analyzes 80 review articles were analyzed to gather relevant information on the research topic. However, after applying the exclusion criteria, the number of review articles was reduced to 26 studies from various disciplines, including computer science, engineering, and policy, to identify common themes and gaps in the literature. The findings suggest that while there has been significant research on the topic, there is still much work to be done to address the unique challenges of securing smart cities. The review highlights the need for interdisciplinary collaboration and the development of innovative solutions that can adapt to rapidly evolving threats. Overall, this systematic review provides a comprehensive overview of the current state of knowledge on smart city cyber security and offers insights that can inform future research and policy decisions.

Keywords: Cyber security; Smart city; Systematic review; Data privacy; Urban governance; IoT

Abbrivations: AI: Artificial Intelligence; CBT: Cognitive-Behavioral Therapy; COT: Cloud of Things; CO_2: Carbon Dioxide; CPSs: Cyber Physical Systems; DDoS: Distributed Denial-of-Service; DOS: Denial of Service; ECC: Elliptic Curve Cryptography; ECU: Electronic Control Unit; GDP: Gross Domestic Product; GSM: Global System for Mobile Communication; HSCCA: Hybrid Smart City Cyber Security Architecture; ICT: Information and Communications Technology; IDPS: Intrusion Detection and Prevention System; IoT: Internet of Things; PICs: Physical Independent Components; RFID: Radio Frequency Identification; SLR: Systematic Literature Review; SRC: Sparse Based Classifier; WSN: Wireless Sensor Networks

INTRODUCTION

A smart city is an urban area that uses technology and data to improve the quality of life for its citizens. Smart cities leverage existing infrastructure, such as Internet of Things (IoT) networks, to collect data on the environment and provide tailored services that meet the needs of their population. These services may range from improved energy efficiency, efficient transportation, and the public safety of users to health care, governance, and education [1]. Smart cities also have the potential to reduce waste and pollution, increase civic engagement, and create economic opportunities.

Received:	05-January-2024	**Manuscript No:**	IPBJR-24-18845
Editor assigned:	08-January-2024	**PreQC No:**	IPBJR-24-18845 (PQ)
Reviewed:	22-January-2024	**QC No:**	IPBJR-24-18845
Revised:	03-February-2025	**Manuscript No:**	IPBJR-24-18845 (R)
Published:	10-February-2025	**DOI:**	10.36648/2394-3718.12.1.117

Corresponding author: Halla Alharbi, Department of Information and Computer Science, College of Computing and Mathematics, Dhahran 31261, Saudi Arabia, Tel: 966568385224; E-mail: halaa.alharbi12@gmail.com

Citation: Alharbi H (2025) Smart Cities Security: Systematic Review. Br J Res. 12:117.

Copyright: © 2025 Alharbi H. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

© Under License of Creative Commons Attribution 4.0 License
This article is available in: https://www.primescholars.com/british-journal-of-research.html

A smart city is designed as a city with strong connections between its physical infrastructure, infrastructure for information technology, and social and business infrastructure, with the ultimate aim of strengthening the overall intelligence network of the city. Smart cities are huge, sensitive, interconnected, and dependent technologies encumbered with many technical, institutional, economical, and social challenges and issues [2].

The evolution, operation, and adaptation of smart cities are faced with myriad issues and challenges that stem from the ever-changing individual requirements, the necessity of stakeholder collaboration, the demand for user-friendly jointing, as well as the increasing concerns of security, privacy, and safety. These multidimensional aspects depict a wide range of economic and investment considerations, which further boost the dynamism of building and sustaining smart cities. With a focus on the economic and investment dynamics of smart cities, these cities endeavor to optimize the allocation of resources, improve technological innovation, and attract businesses. By leveraging advanced technologies using data-driven approaches, these cities anticipate the creation of an ecosystem that assists and encourages entrepreneurship, upgrades productivity, and stimulates sustainable economic growth. Thus, it is necessary to balance resource allocations, making investments crucial to attaining long-term economic viability while meeting the evolving needs of citizens and businesses [3].

Security is an essential aspect of protecting sensitive information and ensuring the safety of individuals and organizations. It involves implementing measures to prevent unauthorized access, use, disclosure, modification, or destruction of data. There are various types of security, including physical security, network security, information security, and cyber security. Physical security involves securing facilities, equipment, and personnel, while network security involves securing computer networks and systems. Information security involves protecting information from unauthorized access, use, or disclosure. Cyber security involves protecting computer systems and networks from attacks such as malware, viruses, and phishing scams. It is crucial to have robust security measures in place to safeguard against potential threats and ensure the safety of individuals and organizations.

This research is about a Systematic Literature Review (SLR) of cyber security for smart cities and provides a deeper understanding of various types of securing it. This systematic review methodology provides a comprehensive and thorough evaluation of the current state of smart city cyber security, identifying areas of strength and areas for improvement [4]. Through an evidence-based approach, the methodology examines existing literature and research studies, collecting data and analyzing findings to form a comprehensive evaluation of the current state of smart city cyber security. The evaluation can then be used to inform decision-making, allowing for the development of effective strategies and policies to improve city cyber security and protect citizens from cyber threats. Specifically, the research aims to address how these characteristics change the nature and relationships between the government and the city's citizens and whether the smart city has effective countermeasures to enable real-time and intelligent decisions for various city functions and citizen needs.

Problem Statement

The main purpose of smart city cyber security is to protect the digital infrastructure of cities from cyber threats and malicious attacks. Smart city cyber security ensures that citizens, businesses, and government entities have a secure digital environment to share information and interact without fear of hacking or data theft. Smart city cyber security helps protect citizens from identity theft, data breaches, malware, and other cyber-related threats while providing access to the latest technologies and services [5]. By investing in smart city cyber security, cities can ensure the safety and security of their citizens and protect their valuable digital assets.

A systematic review of smart city cyber security is a comprehensive assessment of the current state of smart city cyber security. It examines the existing literature and research that is available on the topic in order to identify the key strengths and weaknesses of current approaches. This review enables an understanding of the current state of cyber security in smart cities, identifies areas where improvement is needed, and informs the development of effective cyber security strategies.

Research Aim and Objectives

The aim of this research is to provide a systematic review of smart city cyber security with a view to providing policies and structures for government and citizens to attain the overall effectiveness of smart cities. The objectives to achieve this aim are:

- Review the most current state of smart city cyber security, including the technologies, data privacy, strategies, and regulations in place.
- Analyze the most recent papers on cyber security for smart cities in order to identify key trends and best practices.
- Design the important questions for the research to help us provide recommendations for improving smart city cyber security, including policies, regulations, technologies, and strategies.

Research Methodology

The unprecedented proliferation of Internet of Things (IoT) services has sparked increasing demands for new and creative products for the applications of smart cities. Smart cities, in view of providing the basic requirements of businesses, institutions, and citizens, provide adequate and efficient urban services. These services can be expanded in different fields such as transportation, environment, health, tourism, management, power, and the safety of homes [6]. Though smart cities possess myriad advantages for the environment, citizens, and businesses, they are exposed to many cyber-

security threats that make creating a security system an uphill but attainable task.

The security of smart cities implies data maintenance and the prevention of cyber-attacks. This systemic literature review will answer the following research questions:

- What are some of the most significant cyber security threats facing smart cities, and what are some potential strategies for mitigating these threats?
- Does the smart city have effective countermeasures to enable real-time and intelligent decisions for various city functions and citizen needs?
- What are the implications of smart city cyber security for urban governance, policymaking, and citizen participation?

Research structure this research is structured into 5 chapters:

Chapter 1: Introduction: provides a precise but comprehensive introduction into the search paper. It further explains the aim and objectives of this systematic review and provides the research the research questions this review seeks to answer.

Chapter 2: Related literatures: This chapter provides an exhaustive review of existing publications from verified sites. It constructively and convincingly provides the summary of the work of researchers in this field.

Chapter 3: Systematic review methodology of smart cities security: This chapter of the review explains the method employed in carrying out this review.

Chapter 4: Results and analysis: This chapter explains the outcomes and the findings of this review.

Chapter 5: Conclusion: This summarizes the findings and draw conclusions based on the review.

References: This provides the list of materials consulted, arranged in an alphabetical order

A systematic review is a type of research study that involves analyzing and synthesizing multiple studies on a particular topic. The goal is to provide a comprehensive and unbiased summary of the available evidence, allowing researchers to draw conclusions about the effectiveness of various interventions, treatments, or strategies. Systematic reviews are valuable because they provide a high level of evidence that can be used to inform clinical practice, policy development, and future research. By analyzing multiple studies, systematic reviews can identify patterns and inconsistencies in the evidence as well as highlight areas where further research is needed. People conduct systematic reviews in many different fields, including medicine, psychology, education, and the social sciences [7]. For example, a systematic review might be conducted to evaluate the effectiveness of a particular medication for treating a specific condition or to examine the impact of a particular teaching method on student learning outcomes. To conduct a systematic review, researchers follow a rigorous and standardized process. This typically involves defining a research question, identifying relevant studies, screening and selecting studies based on predefined criteria, extracting data from each study, and synthesizing the results. Overall, systematic reviews are an essential tool for evidence-based practice and research, providing a comprehensive and reliable summary of the available evidence on a particular topic.

Systematic Review Types

A systematic literature review is a methodical and comprehensive approach to identifying, evaluating, and synthesizing existing research evidence relevant to a specific research question or topic. It is an essential tool to inform evidence-based decision making, policy development, and clinical practice. The objective of this systematic literature review is to critically appraise and synthesize the available evidence on the effectiveness of Cognitive-Behavioral Therapy (CBT) in the treatment of depression in adults. There are different types of systematic literature reviews that can be conducted, depending on the research question and objectives. Some of the common types:

Narrative review: This type of review involves a comprehensive search of the literature, but the analysis and synthesis of the findings are done in a descriptive and narrative manner. A narrative review involves a comprehensive search of the literature, followed by a critical evaluation and synthesis of the evidence to provide a comprehensive overview of the topic [8]. The review may include both primary and secondary sources, including books, articles, reports, and other relevant publications

Meta-analysis: Meta-analysis is a statistical method used to combine the results of multiple studies on a particular topic or research question. The objective of meta-analysis is to produce a summary estimate of the effect size or outcome of interest by pooling the results of individual studies. The process of meta-analysis involves a systematic and comprehensive search of the literature to identify all relevant studies, followed by a rigorous screening and selection process to identify high-quality studies that meet the inclusion criteria. The data from the selected studies are extracted and summarized using statistical methods to produce a combined effect size estimate.

Systematic review with or without meta-analysis: This type of review involves the same steps as a narrative review, but the findings are synthesized using a structured approach. A meta-analysis may or may not be included in the synthesis of the findings, depending on the availability and quality of the data. Basically, a systematic review typically involves a rigorous and systematic search of multiple databases, followed by a thorough screening and selection process to identify relevant studies. Quality assessment and data extraction are then conducted on the selected studies to evaluate the risk of bias and extract relevant data for analysis [9].

A scoping review is used to identify the extent of research on a particular topic and to determine the key concepts, theories, sources of evidence, and gaps in the research literature. The main purpose of a scoping review is to map the

existing literature in a particular field, highlight the key findings, and identify gaps and areas for future research. The scoping review involves a systematic and comprehensive literature search, followed by a rigorous screening and selection process to identify relevant studies. Unlike other types of systematic reviews, a scoping review may include a wider range of study designs, including qualitative, quantitative, and mixed-methods studies. The goal is to identify relevant studies that provide insights into the breadth and depth of the literature in the field.

Systemic Review for Smart Cities Security

Smart cities require a uniform IoT architecture based on the three-layer and generally accepted architecture, divided into four layers. The perception layer, also known as the sensing layer, recognition layer, or edge layer, is responsible for data collection and transmission from things in the real world to the network layer for further processing. The network layer is the core layer of the IoT architecture, which relies on basic networks such as the Internet, WSNs, and communications networks to transmit data and connect smart things, network devices, and servers. The support layer provides support for intelligent computing techniques, and the application layer provides intelligent and practical services or applications to users based on their personalized requirements [10].

Modern smart cities are a complex organism made up of five interconnected (yet independent) planes: The sensing, communication, data, security, and privacy planes form the system's backbone, while the application plane provides its residents with the advantages of smart cities through a wide range of services like smart lighting, smart transportation, and smart driving. The majority of recent smart city implementations now include a sixth abstraction plane that ensures interoperability among individual applications in order to take advantage of the synergies already present among various applications, making significant progress toward the realization of a uniform smart city ecosystem.

Smart Cities Related Literate: A General Overview

Due to its strong realistic demand and practical foundation in an increasingly urbanized world, the idea of a "smart city" has gained interest in both academic and industrial disciplines during the past two decades. More than half of the world's population currently resides in urban areas, and it is anticipated that this percentage will reach 66 percent by the year 2050, putting an undue strain on the environment, energy supply, and living standards. A rising number of cities around the world have started to build their own smart plans in an effort to address these issues, promote citizen well-being, spur economic growth, and manage modern cities sustainably and intelligently. Cisco revealed a $1 billion investment in smart cities in 2017. China, the country with the largest population in the world, has more than 200 smart city projects ongoing [11]. Unsurprisingly, a city's infrastructure is embedded with billions of gadgets that, through a variety of applications, such as smart environments, smart homes, smart government, and smart healthcare, can be mutually advantageous for the residents.

Modern smart cities are a complex organism made up of five interconnected (yet independent) planes: The sensing, communication, data, security, and privacy planes form the system's backbone, while the application plane provides its residents with the advantages of smart cities through a wide range of services like smart lighting, smart transportation, and smart driving. The majority of recent smart city implementations now include a sixth abstraction plane that ensures interoperability among individual applications in order to take advantage of the synergies already present among various applications, making significant progress toward the realization of a uniform smart city ecosystem.

Globally, the United States and Europe are leading the way in smart city development. With the aid of information technology like the Internet of Things (IoT), cloud computing, big data, and geographic information systems, it is important to encourage the intelligent transformation of urban planning, construction, management, and services. The smart city has been evolving in two directions for a very long time. First, there is the incorporation of information technology into urban planning, or the building of a digital metropolis. The development of the urbanization process comes in second.

Information technology is one of the main forces behind the creation of the smart city. To address the issue of urbanization, most nations and cities place an emphasis on creating new information infrastructure and employing cutting-edge technological instruments. New infrastructure like the internet and mobile communication networks is the main focus of smart city construction at the moment. Its intelligent urban services, which enhance resident quality of life while supporting the optimization of the urban spatial structure, include police early warning, real-time query of public transportation information, intelligent traffic signals, intelligent parking, and telemedicine.

The perception layer, communication layer, support layer, and application layer are the four components that make up the complicated, multi-level, and methodical project that is building the smart city. Among these, the IoT-based perception layer serves as the basis for a number of smart city operations. Information gathering and environmental monitoring of infrastructure are made possible by sensor technology, Radio Frequency Identification (RFID), embedded system technology, and other sensing devices in IoT technology [12]. The information from intelligent buildings, smart homes, and the internet may all be found in the communication layer, which can be thought of as a "three-network integration" communication information platform.

The IoT perception layer, which can be connected to sensors through some devices and can realize intelligent control of large-scale things through advanced feedback automation technologies like cloud computing and intelligent recognition, is the most crucial and complex of the four layers that make up a smart city. IoT enables intelligent location, identification,

tracking, monitoring, and management by connecting any device to the internet in accordance with the agreed-upon protocol and exchanging information *via* information gathering equipment. Although the IoT makes life and work more convenient for individuals, it still has significant flaws. Many important IoT technologies' standard specifications are still in the early stages at this time. Devices used in Wireless Sensor Networks (WSN) may not be able to withstand all attacks, putting users' location, finances, and other private information at risk of leakage. According to some research, there are six characteristics of smart cities, which are mentioned in **Figure 1**.

Figure 1: An overview of the smart city.

Smart cities are characterized by six key features that are designed to enhance the quality of life for residents, improve sustainability, and promote economic growth, which are mentioned in detail below:

Smart government is involved in decision-making and public services in collaboration with various stakeholders. The government is being mediated by Information and Communication Technologies (ICT) [13]. To keep the decision and implementation processes transparent, smart government is critical to bringing smart city initiatives to citizens.

Smart economy is concerned with improving business life, facilitating, and accelerating the discovery of business services, participating in urban development, increasing GDP, and creating jobs.

Smart people can build a smart economy, a smart education system, and a smart transportation system. Many indicators, such as level of education, academic and technical degrees, and additional training, as well as the ability to communicate in more than one language, can be used to assess smart people.

Smart mobility is concerned with the movement of people or goods within cities, from one location to another, and throughout the world, aided by a safe transportation system and ICT accessibility [14].

Smart living improves one's quality of life. As a result, smart living is defined as providing a better life for citizens through health care, safety, housing quality, social cohesion, and other societal activities.

Smart environment is one that is designed to improve sustainability, clean energy, clean air, and a clean waterfront. Environmental conditions can aid in the development of a smart city by reducing air pollution, water pollution, and CO_2 emissions. As the core concept of smart cities, developing sustainability and managing resources rely on technology.

MATERIALS AND METHODS

The Architecture of a Smart City

The architecture of a smart city is the essentially a wide-scale distributed system with an intrinsically complex and decentralized system. In general, smart city architecture can be categorized into four layers, as shown in **Figure 2**.

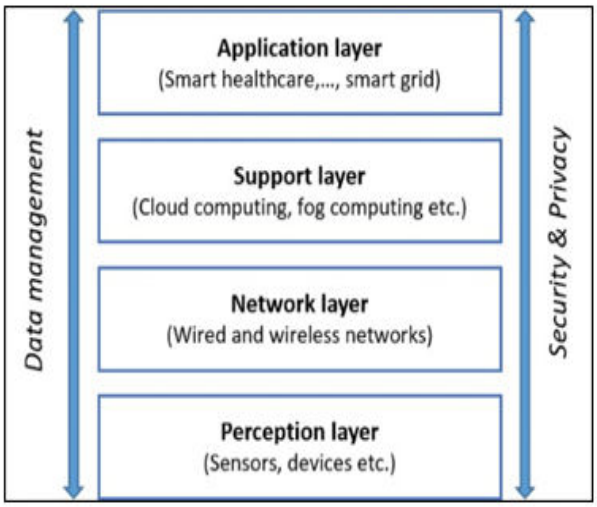

Figure 2: IoT based architecture for a smart city.

Perception layer: This is called sensing layer, recognition layer or the edge layer. It is the lowest layer in the architecture of smart city. This layer is used basically for the collection of data from things such as heterogeneous devices and Wireless Sensor Networks in the virtual world and the transmission of the acquired data to network layer for processing.

Network layer: This is the main part of the smart city IoT architecture. It relies on basic networks like Internet, WSNs and communication network. The main duty of this layer is the transmission of data collected from the perception layer and the use of the same to connect smart things, network devices and servers.

Support layer: The support layer works together with the application layer, by providing required supports for the use of diversified applications through intelligent computations such as cloud computing, edge computing, fog computing and other associated computations [15].

Application layer: This is the top-most layer and is saddled with the responsibility of providing intelligent and feasible services or personalized applications as requested by the users of smart cities.

Applications in the Smart City

In the building of smart cities, one of the objectives is to develop an all-around beneficial residence by focusing on the various closely-related aspects of the users. These aspects include, but are not limited to, energy, environment, industry, standard of living, and associated services. The various applications in the smart city architecture are exemplified in **Figure 3**.

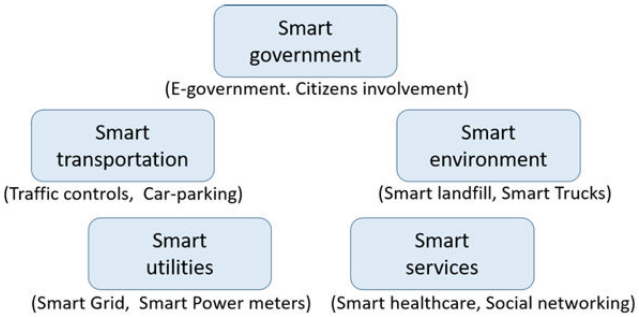

Figure 3: Application in smart cities.

Smart government: Smart government plays a major role in the smart city. The primary role of smart government is to improve service to citizens and community members by interpolating data, organizations, proceedings, and physical infrastructures based on information technology. With smart government, citizens have the freedom to be involved in policy making, public decisions, and overall city planning, with the aim of improving city efficiency while simultaneously improving information transparency. For instance, e-government allows users within the smart city access to government services like applications to use the conference center, payment of bills, and communication of challenges or displeasure.

Smart transportation: Within the city, transportation infrastructure plays a major role. The aim of smart transportation is the provision of improved and efficient transportation systems. Specifically, smarter transportation networks will better serve users by ensuring safety, smooth movement, and dependability. Smart transportation utilizes transport-oriented mobile applications that enable city users to plan their movements by finding the fastest and most viable routes [16]. Other useful applications in smart transportation facilities are license recognition systems, car-parking searching, driver's passports, and time-frame predictions.

Smart environment: The centrality of the smart environment is erecting structures that are environmentally sustainable. Through the application of technical management tools, a smart city is designed to be able to monitor and effectively utilize energy consumption, improve air quality, enhance structural dependability, minimize traffic congestion, and effectively manage generated waste. With the technological innovation implemented in the smart city, prediction of future natural disasters is made easy.

Smart utilities: The main essence of smart utilities is the judicious use of city resources such as water and gas while improving economic growth and environmental protection. Smart metering, which is a smart utility application, is widely applied within smart grids to monitor the distribution of energy resources [17]. In a smart city, the management of resources and reduction of energy loss are made possible *via* smart water meters and smart light sensors.

Smart services: The importance of smart services to users within the smart city is inexhaustible. For instance, with the help of intelligent healthcare applications, it is easy to monitor the health of users through wearable devices and medical sensors. Also, some smart services can create comfortable, intelligent, and energy-saving living environments *via* the use of smart home appliances. On a final note, social networking, e-entertainment, e-shopping, and other smart services have significantly improved the convenience of users within the smart city.

Security and Privacy of Smart City

The security and privacy concerns of smart cities are more germane that the technological phenomena seeing that the demand for smart cities is consistently on the increase globally. Hence the need for researchers to pay more keen attention to the security and privacy of smart cities to enrich further studies with respect to this field of study. Batty, et al., in their study discussed smart cities as a top-notch information and communication technologies and mentioned the present urban problems and modern technologies. They gave further clarifications to the risks and uncertainties associated with smart cities by identifying six city scenarios identified as smart. In another study, Petrolo, et al., gave insights into the basic requirements, the benefits and challenges facing the smart city [18]. The study brought to fore the new version of Cloud of Things (CoT), as a synergy between the internet of things as a technology, and the science of cloud computing by discussing service delivery within smart cities based on the science of cloud of things.

Elmaghraby AS and Losavio MM carried out their study on the cyber security challenges in smart cities: Safety, security, and privacy. The study examined privacy and security concerns of smart cities by providing a model that shows the interaction between the major elements (servers, people, and things) of smart cities. Another study by Bartoli, et al., Bartoli and colleagues explained the regulations surrounding the violations of security and privacy of smart cities. They explained that these regulations are not in consonance with the importance and criticality of security and privacy issues of smart cities.

Doubtless, the benefits of smart cities to its users are high; however, users are bothered about the security of their data being transferred over non-secure channels. This makes it a necessity that secured communication channels must be provided and integrated to ensure the safety of media movement over wireless networks. Ahmed KB et al., in their own study discussed the privacy trade-off with smart city. Ahmed and colleagues explained the downside of privacy and security violations that may occur in the smart city. The internet doesn't forget; hence, users of smart cities must pay a close attention to the kind and volume of personal data they share. Hence, planners, designers and analysts of smart cities must integrate effective protection measures to secure the data of users and prevent them from security breaches. The technologies of cyber-infrastructure for smart cities must be determined during the design process and forecast the city response.

The change of a city from being connected to being smart can be an uphill tasking and a very sensitive one especially on security details as it implicates high level of dependency and interconnectivity across all layers of the smart city. These layers include data/information, technology, application, and the infrastructure. At these layers, it is germane to understand the security challenges and related violations involved a making a smart city. These are identified below:

Infrastructural security in the smart city: There are several vulnerabilities, intricacies, and risks associated with the cyber infrastructure used in smartening up a city. These modern cyber-infrastructural structures within the physical space of a smart city are massively being used but there is no adequate forecast into their vulnerabilities and threats. On a general overview, deliberate and accidental threats to the security infrastructure of smart cities lead to varying degrees of consequences dependent on the maturity and smartness of the city.

The city's urban infrastructure, such as electricity supply, water distribution, layouts of streets, buildings, and others, faces multiple security threats and breaches depending on the physical cyber components, such as:

- **Cameras:** Smart cities are laced with private and public cameras with different degrees of protection using encrypted protection and/or password protection. A breach of these public and private cameras creates unhealthy infiltrations and violates users' privacy.
- **Communication networks:** Cyber-physical objects are linked together with the several communication technologies of the smart city. These communication technologies include Wi-Fi, 4G/5G, Radio Frequency Identification (RFID), and the Global System for Mobile communication (GSM), among others. These communication technologies have peculiar security concerns that must be understood and integrated into the smart city communication system. This implies that communication platforms must be constructed bearing in mind the tendencies of security breaches, hence the need for their security.
- **Building management systems:** Most often than not, designers and developers of these systems focus more on service delivery and pay little or no attention to cyber security breaches. Hence, developers of such systems do not build these systems to trigger notifications to end users in cases of security violations. This lack of response to the vulnerabilities of these systems results in unsecured building management systems.
- **Transport management systems:** A breach in the transportation systems, especially air transportation or train transportation, leads to catastrophic damages. The entire control systems of these transportation systems must be secured, as weak or no security leads to long-hour traffic jams, daylight robbery, and hijacking when the control systems of traffic lights, road signs, and speed limits are tampered with. Fundamentally, urban infrastructure is an integration of Cyber Physical Systems (CPSs) and Physical Independent Components (PICs). The cyber physical components comprise objects like sensors, computing elements, networking elements, etc. The main tasks to be accomplished by CPSs in smart cities are data collection, running on data using the most viable processes, and controlling physical components.

Threats to the security of urban infrastructure in the smart city: As cities become more connected and technology-driven, they are increasingly referred to as "smart cities." Smart city infrastructure is designed to improve the quality of life for residents and enhance the efficiency of urban services. However, with the rise of smart cities come new threats to urban infrastructure security. These threats can include cyber-attacks, physical attacks, and natural disasters, among others. The consequences of a security breach in smart city infrastructure can be severe, potentially affecting public safety, disrupting essential services, and causing economic damage [19]. Therefore, it is essential to identify and mitigate potential threats to the security of urban infrastructure in smart cities. Here are some of the threats:

- **Eavesdropping:** This is the implanting of eavesdropping tools like chips into the specific networks of smart cities for the purpose of spying on channels of communication, monitoring and capturing traffic behavior, and getting the network map. Eavesdropping poses great threats as it leads to the partial or total breakdown of integrity and confidentiality, thereby causing financial and personal losses.
- **Thefts:** Thefts in smart cities are acts of theft of intangibles like sensitive data or information, personal log-in details, software, and tangible elements like smart phones, laptops, and tablets, as well as technological equipment. This act of theft breaks down the availability and confidentiality of systems, leading to financial losses.
- **Denial of Service (DoS):** A denial of service is an attempt to overburden system connections until there is a blockage in the connection. DoS attacks the system's availability to create a blockage or breach in the connection. Other forms of threats can be caused by a crash of software, hardware failure, significant environmental change, or vendors' and manufacturers end of support. These threats affect the integrity, usability, and availability of the system infrastructure, which causes a decline in production and service delivery.

Data/Information privacy in smart cities: The functionality of smart cities depends on a large volume of real-time data and associated innovations. The privacy of smart cities is made feasible by protecting five privacy-related issues, which are: Identity protection, which means the protection of personal and confidential data; the protection of individual areas and properties of users; spatial protection, that is, tracking of real-time location of users; communication protection, which implies the protection of users lines of communication from eavesdropping; and trading protection, which involves the protection of all purchases, exchanges, and financial queries of users in the smart city.

Systematic Review Methodology of Smart Cities Security

Systematic reviews are a complex research method that goes beyond simply collecting data and carrying out analysis. It involves a robust research process that encompasses the collection, synthesis, and analysis of a variety of literature. There are several components that contribute to the successful implementation of a systematic review. These include the selection criteria, search process, and data extraction and analysis. These key components are discussed in greater detail below. As mentioned there are four types of systematic literature reviews that can be conducted: Narrative reviews, meta-analyses, systematic reviews, which is the approach of this research, and lastly, the scoping review. The descriptive systematic review approach and type of domain review were used to conduct the research.

To achieve the aims of this research, a systematic review approach was adopted to review the most current state of smart city cyber security, including the technologies, strategies, data privacy, and regulations in place; design the important questions for the research to help us provide recommendations for improving smart city cyber security, including policies, regulations, technologies, and strategies; and analyze the most recent papers on cyber security for smart cities in order to identify key trends and best practices. The review will provide an up- to-date understanding of the current state of cyber security in smart cities and suggest.

Research Strategy

One of the fundamental goals of this study is to be as inclusive and comprehensive as possible. However, reflecting the fast pace of digital transformation, the search is restricted to more recent publications dated from 2016 onwards and to studies with full text available in English, which included the phrases ‘smart city security’ and ‘systematic review’ for cyber security of smart cities, with the use of the "AND" Boolean operator alongside the keywords to provide a result with all keywords as connected. The research has been done using the descriptive systematic review method.

The protocol is based on the SLR guidelines for the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). The search was run on March 19, 2023. The research process is a systematic approach to investigating and answering questions about a particular topic or phenomenon. It involves a series of steps that are designed to help in identifying a research question, gathering and analyzing data, and drawing conclusions based on the findings, as shown in **Figure 4**.

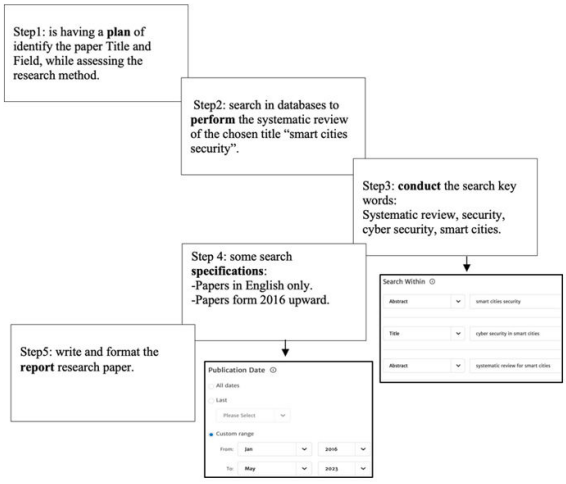

Figure 4: Research process.

The research has taken a few steps to reach its goal. Begins with a review of the existing literature on the topic and specifies the research questions. The primary goal of this research is to identify and present the current state of smart city security in existing research and to assist in determining the direction of future research by addressing the three research questions listed below:

Question 1: What are some of the most significant cyber security threats facing smart cities, and what are some potential strategies for mitigating these threats?

Question 2: Does the smart city have effective countermeasures to enable real-time and intelligent decisions for various city functions and citizen needs?

Question 3: What are the implications of smart city cyber security for urban governance, policymaking, and citizen participation?

Secondly, for computer science research papers, Digital Library (DL) sources were consulted. Utilizing pre-defined keywords that were indicative of the research subject, a search string was created utilizing Boolean operators, key phrases, and synonyms to retrieve all pertinent papers. The main search engine used is Google Scholar. The databases used in this SLR were the Association of Computing Machinery Digital Library (ACM DL), ResearchGate, Springer Open, Science Direct, The Multidisciplinary Digital Publishing Institute (MDPI), the journal and magazines of IEEE Xplore, Hindawi and Journal Storage (JSTOR). To filter the results, the search string was matched to pre-existing parameters in the digital library’s search engines [20].

Searches were conducted to see whether the title, abstract, keywords, and complete text had any terms that matched the search phrase. The search papers were from January 2016 to May 2023. Inclusion criteria were applied manually to the studies collected according to the predetermined search criteria until no further studies met them. The **Figure 5** shows the number of the 80 collected studies from each digital library.

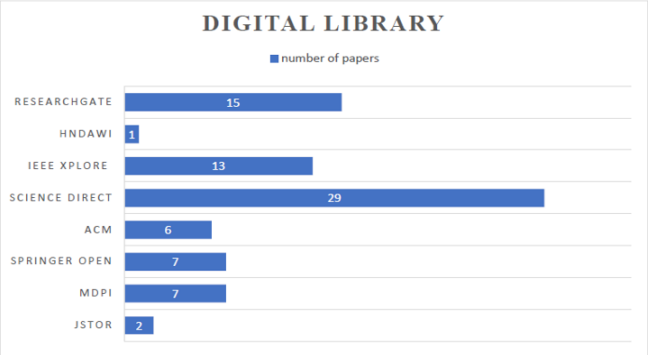

Figure 5: Number of papers in each Digital Library (DL).

Inclusion and Exclusion Criteria

The search results are evaluated against predefined inclusion and exclusion criteria. As for inclusion criteria, reflecting the fast pace of digital transformation, the search is restricted to more recent publications dated from 2016 onwards. Secondly, studies that reference smart cities and technology interventions relevant to security while focusing on cyber security Also, studies that report primary data (qualitative studies) can use qualitative methods; we included systematic review papers on similar topics. All of that included clear descriptions of methods and results.

As for the exclusion criteria, this research excluded study types that are gray literature, dissertations or theses, reviews or published abstracts, studies that were not published in English and studies that are not considered peer-reviewed. Following the scanning, check each study's availability and continue with the papers that we were able to download. Lastly, continue with the 26 papers that we are able to analyze based on our questions. Continue with **Figure 6** that shows the number of the 26 downloaded peppers from each database after the inclusion and exclusion criteria in each database.

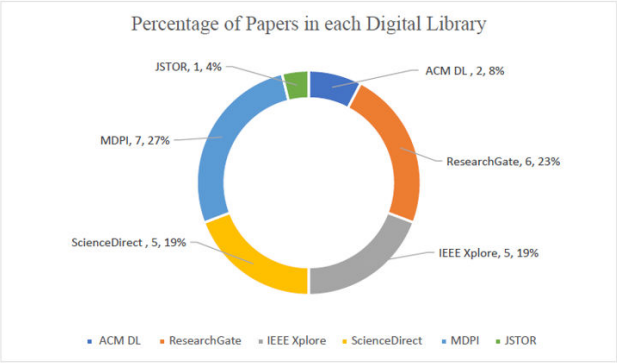

Figure 6: Percentage of downloaded papers after inclusion exclusion criteria in each Digital Library (DL).

Applied Systematic Review Methodology on Smart Cities Security

The screening phase aimed to verify the records according to the inclusion and exclusion criteria previously defined. After a search using the indicated keywords, 80 documents were originally discovered from eight scientific databases mentioned in 3.2 research strategy. The search was run on the SLR guidelines for the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). PRISMA, is an evidence-based set of guidelines for reporting systematic reviews and meta-analyses. The PRISMA guidelines provide a minimum set of items for transparent reporting of systematic reviews and meta-analyses, focusing on the reporting of reviews evaluating the effects of interventions. The guidelines were developed to improve the quality of reporting of systematic reviews and meta-analyses and to facilitate the critical appraisal and interpretation of these reviews by readers. The PRISMA guidelines consist of a 27-item checklist addressing the introduction, methods, results, and discussion sections of a systematic review report. The guidelines have been updated over time to reflect advances in systematic review methodology and terminology. By following the PRISMA guidelines, authors can ensure that their systematic review or meta-analysis is reported transparently and accurately, which can increase the credibility and reliability of the research findings. Complete with the **Figure 7**.

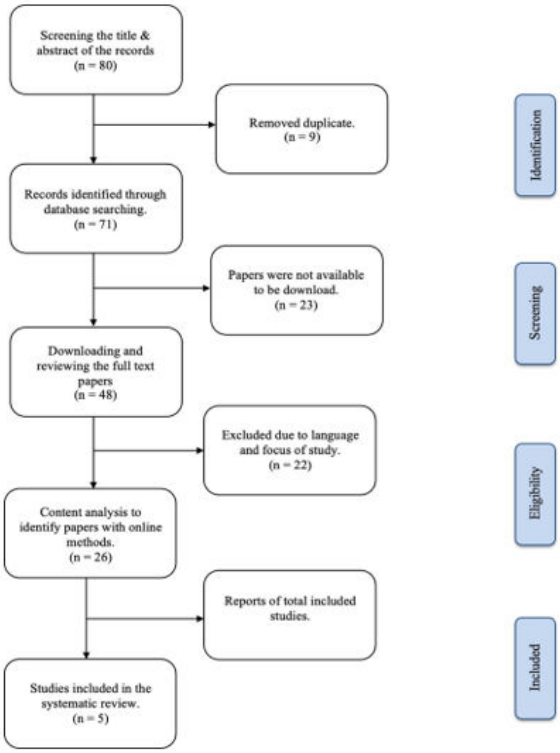

Figure 7: The preferred reporting items for SLR flow diagram.

A total of 26 studies met the criteria for inclusion and exclusion in this review after further screening of the titles, abstracts, introductions, and conclusions of another 48 studies. And 5 out of 26 are the most pertinent survey review articles for presenting the most complete data on the subject.

Research Questions

To assess the quality of each study, three question and answer criteria are developed during this stage, which involves skimming and reading the complete text.

Question 1: What are some of the most significant cyber security threats facing smart cities, and what are some potential strategies for mitigating these threats?

Question 2: Does the smart city have effective countermeasures to enable real-time and intelligent decisions for various city functions and citizen needs?

Question 3: What are the implications of smart city cyber security for urban governance, policymaking, and citizen participation?

By answering this question, this systematic review will provide valuable insights for policymakers, urban planners, and cyber security practitioners in developing effective strategies for securing smart cities and ensuring the privacy and safety of citizens. Cyber security is a critical concern for smart cities as they rely heavily on technology and data to function efficiently. A breach in cyber security can lead to serious consequences such as identity theft, financial loss, and disruption of essential services.

RESULTS

Most Relevant Survey Papers

The systematic review identified 26 studies that met the inclusion criteria. The results showed that technological advancements such as IoT, AI, and big data have significantly impacted safety and security in modern cities. The studies also revealed the challenges associated with implementing and maintaining these technologies. In addition, the review found that cyber security threats pose a significant challenge to smart cities.

Searches with the key search strings in the databases and other search engines from other sources returned a total of 80 articles. After gathering these articles, duplicate articles were removed, leaving us with 71 articles. With emphasis on the titles and abstracts, the 71 articles were streamlined to 48 articles. Which was further reviewed to find the 26 papers that answered the research questions. After a thorough analysis of the 26 articles. In **Table 1**, the focus is on five survey reviews papers that were most relevant to providing the most comprehensive information on the topic.

Table 1: The five relevant survey papers

Title	Author and year	Abstract summary	Methodology
Security and privacy in smart cities: Challenges and opportunities	Cui L, Xie, G, Qu Y, Gao L and Yang Y (2018)	Now that many smart systems have been implemented, security and privacy issues have become a major challenge that requires effective countermeasures. Motivated by these factors, the paper did a survey on the current situations of smart cities with respect to security and privacy to provide an overview of both the academic and industrial fields and to pave the way for further exploration. Then, it discusses the privacy and security issues in current smart applications along with the corresponding requirements.	A survey methodology conducted from the viewpoint of related disciplines (Qualitative).
A Systemic review of technologies and solutions to improve security and privacy protection of citizens in the smart city	Mohammad Hosein Panahi Rizi, Seyed Amin Hosseini Seeno (2022)	In the proper implementation of these cities, a critical challenge is the violation of citizens' privacy and security, which leads to a lack of trust and pessimism toward the services of the smart city. To ensure citizens' participation, smart city developers should adequately protect their security and privacy from gaining their trust. If citizens don't want to participate, the main benefits of a smart city will be lost. This article presents a comprehensive review of smart city security issues and privacy. The paper identifies current security and privacy	Qualitative descriptive systematic review method and type of domain review.

		solutions and describes open research challenges and issues. An output of this study is a systematic map of literature on the subject that identifies critical concepts, evidence, challenges, solutions, and gaps.	
Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects	Saif ur Rehman, Yousaf Bin Zikria, Imran Razzak, Zenera Jalil, Guandong Xu (2022)	Future smart cities are the key to fulfilling the ever-growing demands of citizens. The eventual fate of the world`s betterment lies in its urban environment advancement. Creating sustainable, reasonable space in the world's steadily extending cities is tested confronting governments worldwide. The model of the smart cities rises, where the rights and well-being of the smart city citizens are assured, the industry is in action, and the assessment of urban planning from an environmental point of view. This paper presents a survey on analysing future technologies and requirements for future smart cities. It provides extensive research to identify and inspect the latest technology advancements, the foundation of the upcoming robust era. It also provides a detailed review of the existing future smart cities application frameworks. Furthermore, the paper discussed various technological challenges of future smart cities. Finally, identified the future dimensions of smart cities to develop smart cities with the precedence of smart living.	Quantitative and qualitative method to distributed smart cities' technological and management attributes to view the allied areas' trend and advancements.
Security and the smart city: A systematic review	Chai K Toh (2020)	This systematic review explores the recent literature concerned with new ‘smart city’ security technologies and aims to investigate to what extent these new interventions correspond with traditional functions of security interventions. Ultimately, it proposes three clear categories to categorise security interventions in smart cities: Those interventions that use new sensors but traditional actuators, those that seek to make old systems smart, and those that introduce entirely new functions.	Qualitative methodology of nonnumeric data to highlight the importance of smart cities.
Augmented Reality (AR) and cyber-security for smart cities-A systematic literature review	Nouf M. Alzahrani and Faisal Abdulaziz Alfouzan (2022)	The specific applications of AR and cyber-security technologies have been described in detail in a variety of papers, which demonstrate their potential in diverse fields. Therefore, this systematic review was designed	Followed qualitative SLR methodology

to identify, describe, and synthesize research findings on the application of AR and cyber-security for smart cities. The keynote part of this paper provides an in-depth review of some of the most recent AR and cyber-security applications for smart cities, emphasizing potential benefits, limitations, as well as open issues which could represent new challenges for the future. The main finding that we found is that there are five main categories of these applications for smart cities, which can be classified according to the main articles such as tourism, monitoring, system management, education and mobile.

Security of Smart Cities

Studies shows that the security of smart cities cannot be view singly, that is, securing smart cities must not focus on one aspect of the city seeing that the entire is integrated even though there are distinct layers. According to Chai K, and supported by the research of Khatoun R, and Zeadally S, smart city is likened to the human body with brain, senses, and body parts, though yet interconnected. The security of smart cities must be premised on understanding the specific application (s) that is best suited for each aspect of the city. The security of smart cities will prevent cities from invaders and cyber attackers outside the city walls while also monitoring the infrastructures, applications, services, and interconnectivity of the smart city. According to Chai K, law enforcement, fire rescue services, medical services, transport, communication, and housing services are the six critical services to be protected with utmost priority in the smart city.

Threats of Smart Cities Security Attack

The convergence of the Internet of Things (IoT) and cloud technology that has enabled the emergence of the smart city concept has revolutionized the way cities are managed and maintained. As urban areas become increasingly sophisticated and connected, providing citizens with amenities such as efficient public transit, accessible healthcare, and improved safety, security has become a paramount concern. Unfortunately, with a multitude of new technological components in smart cities, the potential for malicious attack and exploitation rises exponentially. There are many potential security threats to smart cities, including attacks on critical infrastructure, data breaches, cyber-attacks, and physical attacks. There are eight types of cyber-attacks addressed in the 26 included papers which are: Eavesdropping, message injection, radio jamming, DDos, DoS, Man in the Middle, Malware and lastly the sniffing attack. Continue with **Figure 8** to see the percentage of each mentioned attack.

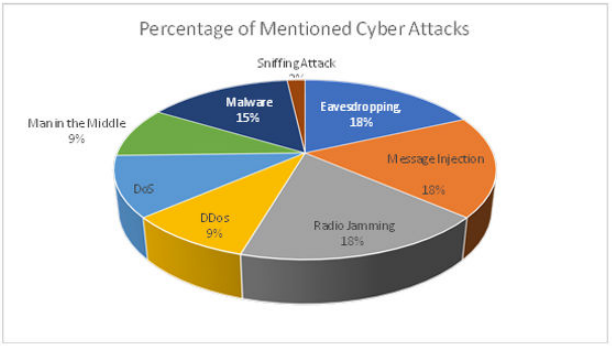

Figure 8: The percentage of each addressed cyber-attack.

Due to the great complexity involved, no examples of smart automation systems achieving system-wide security have been offered. Security concerns continue to be key roadblocks to widespread acceptance and implementation of IoT. In other words, people will not fully embrace IoT if there is no guarantee that their privacy will be protected. And based on the papers they had suggested several techniques to enhance the cyber resilience.

In **Table 2** we explore the threats of security attacks in smart cities and the ways in which they can be addressed, as mentioned in the 26 papers.

Table 2: Cyber-attack mentioned in 26 papers

Number of papers	Security threats	Technology used	Countermeasures
10	Eaves dropping Message injection Radio jamming	Robustness of the system against side channel	**Blacklist mode** **Access control:** Denying unauthorized access to the data.

		threats. platform integrity attestation Radio Access Technology (RAT)	**Encryption:** Protect the content of the data. **Authentication:** Authenticate the source. **Signatures:** Confirm the validity of the data. **Privacy:** Disassociate data from the identify and location of the user.
5	DDoS	Continuous updates for the software	**Cryptography:** RFID blockchain; distributed architecture based on blockchain technique and fog computing. Biometrics; biometric based authentication and key negotiation protocol
6	DoS	Software Define Networking (SDN)	Data encryption (Elliptic Curve Cryptography (ECC))
5	Man-in-the-Middle (MITM)	Block chain technology	Authentication between sender and receiver distributed set of network entities such as: Intrusion Detection and Prevention System (IDPS) Received Signal Strength (RSSI)
8	**Malware attacks:** Worms Ransomware Adware Virus SpyWare Trojan Horses	IoT protection mechanism such as: Authentication and encryption Edge Computing Architecture (ECA) (Edge computing is an extension of cloud computing)	**Access control:** Denying unauthorized access to the data. **Encryption:** Protect the content of the data. **Authentication:** Authenticate the source. **Signatures:** Confirm the validity of the data. **Privacy:** Disassociate data from the identify and location of the user.
1	Sniffing attack	Tagging technique	**Data encryption:** Elliptic Curve Cryptography (ECC)

The studies of Habibzadeh et al., Fan et al., and Lv et al., revealed the major security challenges facing smart cities. Firstly, eavesdropping on communication exchange between sensors and equipment's to users provides cyber-attackers with adequate knowledge to perpetrate their malicious actions. Also, due to the distortion of messages sent to the subsystems, false or incomplete messages are sent to various devices, thereby distorting the sequential operations of the smart city systems. Thirdly, message injection by cyber attackers is also able to interfere with the response time of communication systems, leading to service denial within the smart city. Some messages exchanged and transmitted in the systems may be time-dependent, and a delay in delivery may cause colossal damage.

Tariq et al., Chen et al., and four others, in their studies discussed the identifiable cyber security threats/issues emanating from the cloud is the vulnerability of systems and applications, injection of malware attacks, insider threats, data leakage, and Denial of Service (DoS). Other feasible that can emanate from IoT sensors is remote exploitation, failure of sensors, failed data storage, problems with effective data management, insecure communication, and leakages in confidential data. However, with respect to smart grids, issues like attack on internet-connected devices, infected devices, eavesdropping, privacy, and the vulnerability of protocol can also pop up.

Baig et al., explained the varying type and degrees of physical threats from such systems in the smart city. These physical threats include introduction of data glitches in order to get unverified access into debug interfaces, attack on side channels to expose information or false injection into the ECU to defeat the central locking systems. Habibzadeh et al., Rahouti, Xiong, and Xin, and three others further identified other challenges of smart cities and addressed other issues like man-in-the-middle attack, phishing, and spoofing. When cyber-criminals intercept communication channels with the aim of manipulating data transmission and falsify the action of the operators, this is regarded the man-in-the-middle attack. Spooning involves exposing data by third malicious party sending the same after exposing the security protocol while phishing involves impersonation of trusted and reputable individuals by cybercriminal to gain credible information like credit cards and log in details.

In another study by Cui L, the author identified threats posed by AI in smart cities. Though AI plays significant roles in many intelligent applications like automatic control of trading systems, home appliances and pacemakers, the increasing use of AI spells more danger than succour. For instance, device manufacturers and service providers can utilize technologies for data mining to excessively analyses individual data and be able to extract sensitive information that stands aloof from the primary objectives of its services. Furthermore, cyber-attackers who are proficient with the use of AI are also getting wiser by the day. Cyber-attackers may have a deep understanding on the working of AI. Hackers may comprehend ML-based protection mechanisms; hence, they were trained to be able to adopt targeted approaches than to weaken the training effects and to reduce the reliability of the algorithms.

Countermeasures to Security Breach on Smart Cities

Although the final specific spatial dimensions of smart cities significantly vary, many scholars believe that it is necessary to have different but defined precautionary measures, interventions, and solutions to all forms of cyber threats to guarantee a smoother implementation and process and ultimately a secured smart city. According to the study by Chen et al., author believes that the current cyber security, as countermeasures to security breaches and threats, is still unable to effectively tackle the threats and challenges that smart cities are faced with.

Though smart cities are designed to be secured, the security outfit must be up-to-date to effectively address any form of security threat should any breach arise. In their study, they suggested that the security structure of smart cities must be extensive, based on learning methods, detailed, and possess effective preventive mechanisms for all technological systems in the smart city. This study provides a summarized interpretation of deep learning, cyber security, and the concepts of security and privacy in smart cities. Specifically, Chen and colleagues mentioned deep learning models designed to enhance the privacy and security of smart cities.

These models include Boltzmann machines, generative adversarial networks, convolutional neural networks, recurrent neural networks, and deep belief networks. Habibzadeh et al., provide comprehensive review Radio Access Technology (RAT) devices and block chain technology and its applications in various industries. The authors highlight the potential of block chain technology to improve transparency, security, and efficiency in financial transactions, supply chain management, and healthcare. They also discuss the challenges and limitations of block chain technology, including scalability, interoperability, and regulatory issues. Rahouti, Xiong, and Xin focus on the use of block chain technology in the context of smart cities. The authors highlight the potential of block chain technology to enable secure and transparent data sharing and to facilitate the development of decentralized applications that can improve the quality of life in urban areas. Tariq et al., provide a review of block chain technology in the context of the Internet of Things (IoT). The authors highlight the potential of block chain technology to enable secure and transparent data sharing and to facilitate the development of decentralized IoT applications. They also discuss the challenges and limitations of using block chain technology in IoT applications, including scalability, interoperability, and energy efficiency.

A corresponding approach to these security threats in smart cities was postulated by Belgaum, et al., Mohammad RMA, and Abdulqader and Fard, et al. They designed a threat 'hunting' model based on a Sparse Based Classifier (SRC). The security frameworks suggested by these authors identify the cyber threats to smart cities *via* Opcode, Bytecode, and system call views to suggest ways of addressing, preventing, and tackling these cyber threats. Abosaq in his own research, suggested enforcing data privacy through the tagging technique, which is considered very successful. Data tagging aids in the flow of information and the preservation of individuals' identities, but because it requires a lot of overhead to manipulate, it is not very useful in the IoT due to its limited processing capabilities. This is to say that innovative technologies in smart cities must be integrated into the security framework over a long period of time.

Implications of Smart City

Smart cities are rapidly emerging as a solution to the complex challenges facing urban communities, including population growth, climate change, and resource constraints. These cities leverage the power of technology to optimize critical city functions, such as transportation, energy, and waste management, to improve the quality of life for citizens. However, as the use of technology in urban environments grows, so do concerns about cyber security. The implications of smart city cyber security are vast and far-reaching, affecting urban governance, policymaking, and citizen participation. Smart city cyber security is a critical issue that has significant implications for urban governance, policymaking, and citizen participation. According to Rahouti, Xiong, and Xin, the smart city effort seeks to offer cutting-edge approaches that heavily rely on Information and Communications Technology (ICT) to improve local sustainability in terms of people, government, economics, transportation, environment, and way of life in metropolitan areas.

Based on Hammi et al., smart cities are interconnected cities that employ telecommunications and information technology to improve people' lives. The authors believe that a smart city can be made smart by achieving two primary goals:

Providing an advanced urban infrastructure capable of collecting and processing data using emerging technologies such as smart grid, smart meters, smart buildings, connected objects, and big data to anticipate any anomalies.

Providing smart applications that allow people to engage with the environment in order to minimize CO_2 emissions. Reduced pollution levels will benefit the environment and, eventually, residents' quality of life (e.g., improved health, safer, quicker, cheaper commute).

Urban governance: In the context of communication and building trust amongst devices, the new urban governance models that are present inside the infrastructure of smart cities reveal a variety of new risks to user and network data privacy, confidentiality, the operational integrity, and public confidence inside the smart city infrastructure are crucial elements linked to technical and security governance of smart cities.

In theory, smart city refers to the collaboration of governance institutes and public and private foundations in order to implement and deploy long-term computerized platforms that impose modern technologies such as mobile cloud computing, electronic objects, networks, and intelligent decision-making methodologies. Globally, smart cities attempt to address the major difficulties that the world is now facing, such as climate change, limited resources, urbanization, and rapid population development.

As experimental communication tools with residents, corporations, and other local and national authorities, some municipal governments started e-government initiatives. In addition to internal networks for the management of public institutions, some progressive local governments have created ICT networks for the community that involves all stakeholders. They have been utilizing networks and associated ICT solutions in an effort to improve their decision-making process.

Policy making: Fabrègue and Bogoni support the development of technological procedures that aimed at expanding the scope of IT governance practices. To make policymakers accountable for their decisions not just during deployment stages but also during operation, an ethical dimension must be incorporated into each level of decision making by establishing duties. Transparency at all levels of decision-making is the only way to keep the advantages of smart cities from being overshadowed by distortions caused by biased information. The Internet of Things (IoT) is a key enabler for a wide range of smart applications involving vast data collecting and intelligent decision making.

As a result, in the development of smart cities, the IoT serves as a bridge between sensing devices and the data plane. The Internet of Things (IoT) enables communication between the collection of sensory input and the making of decisions across vast, diverse, and unstructured data. The most crucial design considerations for any individual component of a smart city system are, in fact, security and privacy.

Proposals for IoT-enabled smart city applications must carefully assess the application's environment and societal expectations in addition to the standard security issues to ensure their viability. More study should be focused on other security challenges such maintaining the quality of security services, compatibility across multiple protocols, and safe updates for vast IoT networks. Autonomous or semi-autonomous complex systems with the ability to make cognitive decisions will become more prevalent as our IoT systems gradually transition from "perceptive" to "cognitive".

Citizens participation: A smart city relies heavily on smart government. The goal of smart governance is to enhance the lives of citizens by utilizing information technology to integrate data, institutions, processes, and physical infrastructures. Furthermore, smart governance allows citizens to participate in public choices and city planning, which can enhance efficiency while also enhancing information transparency. e-government, for example, enables citizens to access government services online, such as applying for a conference center, paying bills, and reporting difficulties. Smart cities represent the highest level of ICT innovation. Citizens in smart cities are linked by smartphones and artificial and integrated technologies such as the internet of things, resulting in an unfathomable level of comfort and lifestyle enhancement.

Additionally, smart cities seek to ensure economic competitiveness in metropolitan areas and provide urban residents with more upscale lives.

Ahmadi-Assalemi, Al-Khateeb, Epiphaniou, and Maple, define on their study a smart city as an urban area that uses technology and resources in an inventive, wise, and secure manner to better the lives of its residents, with an emphasis on a range of characteristics that increase the cyber resilience of smart cities.

DISCUSSION

According to researchers, smart cities are cities that utilize Information, Communication Technology (ICT) systems to disseminate information to citizens, improve operational efficiency, and ultimately enhance the quality of public services. The key aspects of smart cities are smart governance, smart education, smart environment, smart homes, smart transportation, smart energy and smart health. The operations of smart cities are faced with series of challenges traceable to the consistent demands from individuals, stakeholders, expressing concerns of security, privacy and safety. These interconnected and complex demands represent a wide range of economic and investment considerations, which ultimately boost the dynamism of building and sustaining smart cities.

One of the most profound expressions of the effectiveness of smart cities is safety and security. The consistent increase in data use and connectivity, they become more prone to cyber threats, privacy breach and associated risks. Thus, cyber security, and data privacy measures are important essentials to earn the trust of users and stakeholders. Also, advanced technologies like surveillance videos, sensor networks, and predictive analytics can be deployed to enhance public safety, emergency response, and disaster management capabilities within the smart city. The security of smart city is an important issue that affects the development and support of these cities as cyber security plays a central role in the development of smart city. The research aims at providing a systematic review for smart cities cyber security with a view to providing policies and structures for government and citizens to attain the overall effectiveness of smart cities.

Information communication and technology is one of the main forces behind the creation of the smart city as a means of addressing the increasing issues of urbanization by creating new information framework and employing cutting-edge technological instruments. The architecture of smart cities with the multilevel and multidimensional functions has four main components which are perception layer, communication layer, support layer, and application layer.

The functionality of smart cities depends on large volume of real time data hence the need for data privacy. This data privacy of smart cities is made feasible by protecting five privacy related issues which are: Identity protection, individual area and property protection, spatial protection, communication protection, and trading protection.

According to Baig et al., major cyber security threats and issues emanating from cloud computing is the vulnerability of systems and applications, injection of malware attacks, insider threats, data leakage, and Denial of Service (DoS). Issues like attack on internet-connected devices, infected devices, eavesdropping, privacy and the vulnerability of protocol are traceable to threats smart grids face within the smart city. Though AI plays significant roles in applications within the smart city like automatic control of trading systems, home appliances and pacemakers, device manufacturers and service providers can utilize technologies for data mining to excessively analyze individual data and extract sensitive information. On the contrary, cyber-attackers who are proficient with the use of AI can weaken the privacy effects of the system and reduce the systems' algorithms.

Nasser H. Abosaq asserted that confidentiality of data and data privacy are the major challenges encountered by citizens in the smart city. He recommended tagging as very effective technique policy enforcement in IoT. In the overall optimization of smart cities, smart applications, Internet of Things (IoT), cloud computing, big data, Wireless Mesh Networks (WMN), wireless sensor networks and many other cutting-edge technologies play vital roles. In the security of smart cities, understanding the possible threats smart cities face is important to establishing a secured infrastructure to fight these threats.

On a final note, the identifiable threats, and challenges smart cities face centres around data privacy breach of individual users and the protection of these smart cities is the responsibility of the government and smart city developers.

CONCLUSION

The concept of smart cities reaches far beyond the scope of this study. Cyber-security is a critical aspect within the newly developing smart sector, with a high priority towards maintaining research goals. As smart cities evolve, they are faced with different degree and kinds of threat which borders around data privacy breaches. This has prompted developers of smart cities to continue to develop countermeasures. This Systemic Literature Review (SLR) was carried out with the aim of evaluating the current state of research on smart city cyber security, with a specific focus on the challenges and solutions related to protecting critical infrastructure, personal data, and public safety.

Studies in this review has revealed that smart cities are designed to be self-sustaining and the cyber security challenges that may arise against can be general, that is, affect the entire smart city or an aspect of the technology of smart city, such as communication, transportation, governance, or business technologies. The operational technologies and the interconnectivity of these technologies in smart cities have proven to give rise to a number of security threats. These threats ranges from loss of privacy and confidentiality, physical threats, systems and applications vulnerability, malware injection attacks, Denial of Service (DoS), malicious insider threats, to data leakage.

Within the smart city, law enforcement, fire rescue services, medical services, transport, communication, and housing services are the six critical services to be protected with utmost priority. The common security threats on smart cities are on infrastructure, communication, and transportation. The common counter measures to security threats and breaches on smart cities vary across different researchers and includes Hybrid Smart City Cyber Security Architecture (HSCCA) framework, Boltzmann machines, generative adversarial networks, convolutional neural networks, recurrent neural networks, to mention but a few. However, the common indicator of all counter measures is the appraisal of the degree and kind of threats and development of a preventive security framework to address these cyber threats in smart cities.

Future Work

The cyber security of smart cities is very germane as it involves the consideration of several findings on technologies, applications, infrastructure and information/data. The emerging integration of these technologies, intensive communication, high complexity and high interdependency, has led to a number of security challenges and these challenges have resulted into series of attacks on the data privacy of users. Hence, the need to enact policies, develop new applications and security framework that will enhance users' data security within the smart city. As researchers carry out their tasks with respect to privacy breaches in smart cities, they must consider the ethical implications of their work with respect to the new security frameworks of smart cities.

This review was carried out with the aim of evaluating the current state of research on smart city cyber security, with a specific focus on the challenges and solutions related to protecting critical infrastructure, personal data, and public safety. Data privacy of the users in smart cities should be a major concern and must not be compromised while designers of smart cities are planning and designing the infrastructure of smart cities. Hence, both government and the corporate sector must work collaboratively to secure users' data from exploitation; else, trust on data privacy of end users might be a daydream. Also, possible future works can be carried out by finding the best privacy rule based on logic, taking into

consideration the penetration rate of the system and accuracy of the architecture, and comparing Edge Computing Architecture (ECA) with other suggested means *via* more possible parameters such as accuracy.

The findings suggest that the implementation of technological advancements requires careful planning and management to ensure their effectiveness in improving safety and security. The review also highlights the need for a comprehensive approach that integrates various aspects of safety and security, including emergency preparedness, access control, risk assessment, and response time.

REFERENCES

1. Alzahrani NM, Alfouzan FA (2022) Augmented reality (AR) and cyber-security for smart cities-A systematic literature review. Sensors. 22(7):2792.
2. Arias O, Wurm J, Hoang K, Jin Y (2015) Privacy and security in internet of things and wearable devices. IEEE Trans Multi-Scale Comput Syst. 1(2):99-109.
3. Baig ZA, Szewczyk P, Valli C, Rabadia P, Hannay P, et al. (2017) Future challenges for smart cities: Cyber-security and digital forensics. Digi Inves. 22:3-13.
4. Barsocchi P, Cassara P, Mavilia F, Pellegrini D (2018) Sensing a city's state of health: Structural monitoring system by internet-of-things wireless sensing devices. IEEE Cons Elec Mag. 7:22-31.
5. Bartoli A, Hernandez-Serrano J, Soriano M, Dohler M, Kountouris A, et al. (2012) On the ineffectiveness of today's privacy regulations for secure smart city networks. Smart Cities Council, Washington, DC.
6. Lo'ai AT, Basalamah A, Mehmood R, Tawalbeh H (2016) Greener and smarter phones for future cities: Characterizing the impact of GPS signal strength on power consumption. IEEE Access. 4:858-868.
7. Batty M, Axhausen KW, Giannotti F, Pozdnoukhov A, Bazzani A, et al. (2012) Smart cities of the future. Euro Phys J Special Top. 214:481-518.
8. Belgaum MR, Alansari Z, Jain R, Alshaer J (2018) A framework for evaluation of cyber security challenges in smart cities. In Smart Cities Symposium 2018. 1-6.
9. Ahmed KB, Bouhorma M, Ahmed MB (2014) Age of big data and smart cities: Privacy trade-off.
10. Catarinucci L, de Donno D, Mainetti L, Palano L, Patrono L, et al. (2015) An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J. 2(6):515-526.
11. Chen D, Wawrzynski P, Lv Z (2021) Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustain Cities Soc. 66:102655.
12. Cui L, Xie G, Qu Y, Gao L, Yang Y (2018) Security and privacy in smart cities: Challenges and opportunities. IEEE Access. 6:46134-46145.
13. Elmaghraby AS, Losavio MM (2014) Cyber security challenges in Smart Cities: Safety, security and privacy. J Adv Res. 5(4):491-497.
14. Fan J, Yang W, Liu Z, Kang J, Niyato D, et al. (2023) Understanding security in smart city domains from the ANT-centric perspective. IEEE Internet Things J. 10:11199-11223.
15. Fard SM, Karimipour H, Dehghantanha A, Jahromi AN, Srivastava G (2020) Ensemble sparse representation-based cyber threat hunting for security of smart cities. Comput Elec Eng. 88:106825.
16. Gil-Garcia JR (2012) Towards a smart State? Inter-agency collaboration, information integration, and beyond. Inform Polity. 17(3-4):269-280.
17. Habibzadeh H, Soyata T, Kantarci B, Boukerche A, Kaptan C (2018) Sensing, communication and security planes: A new challenge for a smart city system design. Computer Networks. 144:163-200.
18. Badouch A, Krit SD, Kabrane M, Karimi K (2018) Augmented Reality services implemented within smart cities, based on an internet of things infrastructure, concepts and challenges: An overview. InProceedings of the Fourth International Conference on Engineering and MIS 2018.
19. Ijaz S, Shah MA, Khan A, Ahmed M (2016) Smart cities: A survey on security concerns. Int J Adv Comput Sci Appl. 7(2).
20. Kabalci Y (2016) A survey on smart metering and smart grid communication. Renew Sustain Energy Rev. 57:302-318.