International Journal of Applied Technology & Leadership
ISSN 2720-5215
Volume 3, Issue 1, January 2024
ijatl@org

An Investigative Review: Smart Grid and Consumer Privacy Concerns

Sandra Moore, ScD

Capitol Technology University (USA)

Richard W. Lightcap, PhD, EdD

Capitol Technology University (USA)

William H. Butler, DSc

Capitol Technology University (USA)

Abstract

Smart grid technology's boundary of impact and security risk ranges from utility services, energy management services, manufacturers, law enforcement agencies, and consumers. As smart technology is deployed at a faster pace than regulation can keep up with as well as identifying vulnerabilities within smart technology; it becomes necessary to better understand what smart technology is currently available. To assist everyday consumers in better understanding how their data is collected, used, analyzed, and the potential implications stemming from the use of their data, we discuss multiple state and international privacy laws and examples of misuse cases.

Keywords: smart cities, smart meter, smart technology, critical infrastructure, cybersecurity, surveillance city

1. Introduction

Smart cities leverage technology and resources to create energy-efficient and sustainable urban centers. The integration of smart grid technology enables capabilities such as load balancing for homes, consumer energy feedback systems, and electric vehicle charging stations. However, the extensive use of data analytics from smart grid technology raises concerns about consumer

privacy and the lack of regulations protecting their data. The responsibility for safeguarding consumer data when companies outsource remains ambiguous, and privacy is often overlooked in the implementation of smart grid technology. While the use of smart technology and Artificial Intelligence (AI) algorithms can enhance system monitoring, they also pose risks of advanced cyber-attacks.

Döbelt et al. (2015) emphasized the importance of understanding consumer privacy concerns within the context of smart grid technology and the level of trustworthiness of entities handling energy data and delivery. Consumers need transparency regarding the use of their data and the potential consequences of data breaches. Therefore, it is crucial for smart grid technology and smart cities to prioritize consumer privacy protection.

In addition, Yang et al. (2021) highlighted the differences in smart city goals and services between regions, emphasizing that technology application does not automatically align with the smart city initiatives. This underscores the need for a comparative analysis of smart grid and smart city technology, as well as privacy concerns, across different regions to help consumers understand how their data is collected, used, and the potential implications of its utilization.

2. Background

2.1. Fundamental Architecture of Smart Grids

In a traditional power grid design power flows in one direction, from the generation facility over the transmission lines delivered to the consumer via distribution utilities. As utility companies integrate modern technologies to meet changing consumer needs, the basic composition of the power grid remains consistent with the original power generation system introduced in the early 1900's (Kessel & Glavitsch, 1986). The traditional power grid design has largely remained unchanged over the years, with adding layered features and protocols on an already aged system, providing threat actors great opportunities for compromise.

Smart Grids represent a framework of distributed and hierarchical network systems that incorporate two forms of transmission technology, Wide Area Network (WAN) and Home Area Network (HAN). WAN, typically used in information technology computing networks, encompasses telecommunications networks that extend over large geographical areas, utilizing technologies such as LTE, 5G, leased lines, or fiber optic lines. On the other hand, HAN refers to an interconnected network of devices within a home, whether wired or wireless, including computers, mobile devices, IoT devices, streaming devices, and smart appliances. The architectural and application standards within the context of Smart Grids are continuing development and analysis, driven by the National Institute of Standards and Technology (NIST) having developed a reference framework, NIST Special Publication 1108rev4, to guide Smart Grid implementations and developments (Gopstein et al., 2022).

With the introduction of smart grid technology, having brought about enhanced efficiency and reliability, but it has also introduced new vulnerabilities to critical infrastructure if not deployed with appropriate security controls (Pillitteri & Brewer, 2014). Implementing cybersecurity protocols for such a complex network of systems may seem daunting, but it is essential to

prevent exposure to cyber-threats and attacks. The National Institute of Standards and Technology (NIST) continues to publish and update guidelines related to smart grid cybersecurity to assess and identify cyber risks and apply appropriate countermeasures.

Smart grids encompass four basic areas: generation, distribution, delivery, and use, each heavily reliant on a series of complex control signal technologies (Butun et al., 2020). Generation involves voltage regulation, governor monitoring of frequency alterations within the grid, and automatic generation control to fine-tune disturbances (Kessel & Glavitsch, 1986). Distribution is maintained through load shedding and advanced meter infrastructure, while delivery occurs through state estimation and volt-ampere reactive methods (Butun et al., 2020; Kessel & Glavitsch, 1986). Finally, the consumption required by consumers is delivered to their homes or businesses.

2.2. Why are smart cities being implemented?

According to the United Nations, more people are moving to cities, and this has led to the adoption of smart city models that increase digitization for efficiency and sustainability (United Nations, 2019). The smart city model is a model which integrates technology and data to enhance the quality of life for citizens within its service area, increase sustainability, and modernise urban services. One proposed model for smart cities is the seven smart components system (7SCCS), which is an ICT-led model that aims to achieve balanced development and emerging structures in smart cities (Mardacany, 2014). The seven components include smart governance, smart economy, smart mobility, smart environment, smart people, smart living, and smart ICT infrastructure. The model proposes that these components work together to create a sustainable and efficient smart city.

The National Strategic Smart City Program (NSSP) in South Korea is a strategy that seeks to establish new technological standards and ecosystems for smart cities. The NSSP aims to create a new technological ecosystem that will enable the construction of smart cities within the South Korean country (Yang et al., 2021). The NSSP focuses upon the development of smart city services that are tailored to the needs of citizens and businesses. The NSSP also aims to establish new standards for smart city infrastructure, such as data centers, communication networks, and sensors.

However, achieving smart city goals is impacted by various factors such as dust, energy inefficiency, aging populations, traffic congestion, large-scale disasters, and administrative inefficiencies. These factors can hinder the development of smart cities and make it difficult to achieve sustainability and efficiency goals. For example, energy inefficiency in old buildings and infrastructure can lead to increased energy consumption and higher costs (Yang et al., 2021). Traffic congestion can lead to longer commute times and increased air pollution. It is also important to note that data privacy and security are not major provisions in the NSSP and other national plans. This is a significant concern as smart city models rely heavily on data collection and analysis. Without proper data privacy and security measures, citizens' personal information could be at risk of being compromised.

3. Review of Literature

The literature lacks indicators of the importance of the necessity of further research on the implementation of technical aspects of smart city deployments and their impact on society (Sharifi et al., 2021). While smart cities promise to improve citizens' lives, it is unclear whether they will actually deliver on this promise. Therefore, more research is needed to understand how smart cities can improve the lives of their citizens. Additionally, the review emphasizes the importance of considering security and privacy from the beginning of the implementation process, rather than as an afterthought. According to Sookhak et al. (2018) this is due to the collection, storage, and real-time analysis of enormous volumes of data making it challenging to efficiently protect security and privacy. Failure to do so can result in data breaches, which can have tangible consequences for individuals, such as the loss of healthcare or geographic records (Sookhak et al., 2018). Furthermore, the review highlights the need to focus not only on security but also on privacy, as metadata can reveal more about individuals when aggregated (Schneier, 2015). Therefore, understanding how to secure smart technology and how data is used in smart cities is necessary to safeguard citizens' data and ensure their privacy.

3.1 Security and Smart Technology

The advanced metering infrastructure [which includes smart meters] is a critical component within smart grid technology. With the criticality of the advanced metering infrastructure, it is paramount to apply security measures to protect it from potential attacks. Acting as a gateway between in-home devices and external entities, a smart meter acts to provide needed and up-to-date information. These smart meters contain three main interface types from which a cyber-related attack can be introduced through the optical, wireless, or cellular interfaces (Butun et al., 2020; Kebotogetse et al., 2021).

3.2. Optical Interface

The optical interface on the smart meter can be attached with a cable to a port on the meter to allow an attacker to use software to analyze and alter meter values. Using this same process, a threat actor could attach a small computing device and initiate an attack to control various portions of the residence or business managed by the smart meter. This type of physical connection attack allows for the bypassing of encryption mechanisms, although it does require physical access to the smart meter (Kebotogetse et al., 2021). An attacker could potentially gain access to sensitive information and manipulate meter values, leading to financial losses for the affected residence or business. Additionally, the ability to control various components of the smart meter system could pose significant safety risks to the occupants of the property.

Furthermore, the physical connection attack not only undermines the encryption mechanisms designed to secure the smart meter but also highlights the importance of physical security measures in addition to cybersecurity protocols (Zhang et al., 2021). This further underscores the need for comprehensive security strategies that encompass both digital and physical aspects to safeguard against potential threats. The criticality to implement a robust and complex

physical security controls and cybersecurity protocols to protect smart meter systems from potential physical connection attacks and the associated risks they pose to the integrity and functionality of the smart meter system.

3.3. Wireless Interface

The wireless interface of smart meters serves as a crucial component for energy consumption calculations and data collection within the Home Area Network. This interface, however, presents a potential vulnerability that can be exploited by malicious actors. By taking advantage of the periodic nature of data collection, an attacker could manipulate the normal network packet transmission, for instance, by obstructing the delivery of these packets. This type of attack could be executed through radio jamming over ZigBee radio frequencies, effectively disrupting communications between the smart meter and the utility service provider (Butun et al., 2020). Additionally, the attacker might engage in eavesdropping to intercept the DLMS/COSEM portion of the network packet, potentially leading to data leakage or loss (Butun et al., 2020; Kebotogetse et al., 2021; Kistler et al., 2009). It is notable such wireless cyber-threats can have significant repercussions, impacting not only the delivery of electricity but also posing risks to consumer data security and privacy. These risks underscore the need for robust security measures to safeguard smart meters and the Home Area Network from potential wireless attacks.

3.4. Cellular Interface

Threat actors can compromise the interaction between the GSM access point and the data control model by eavesdropping on the wireless interface. This type of attack can be executed using a GSM traffic sniffer to intercept and compromise the key, leveraging a ciphertext attack on the GSM protocol (Barkan et al., 2003; Barkan et al., 2008). The consequences of such an attack can be severe, as it can allow the threat actor to connect to the remote terminal unit at the substation and manipulate the electric breakers, causing a power loss. This can result in significant financial losses for both the utility company and the consumers, as well as potential safety hazards. The encrypted data can be exposed using the Barkan-Biham-Keller method recovering the key allowing the threat actor to connect to the remote terminal unit at the substation and altering the electric breakers to initial a power loss (Butun et al., 2020).

To prevent such attacks, we are reminded of the importance of implementing a robust set of security measures and protocols. For instance, the use of encryption and authentication mechanisms can help protect the transmission linking the smart meter and the data control center. Additionally, routine security audits and updates can aid in the identification and addressing of any vulnerabilities in the system. This is also essential to educate consumers and utility companies about the potential risks of cellular attacks on smart meters and the importance of maintaining secure communication channels. By staying informed and taking proactive measures, we can ensure the security and reliability of our smart grid infrastructure.

3.5. Encryption

The implementation of smart grids has led to the introduction of communication protocols aimed at addressing security concerns. Different regions utilize specific protocols, with IEEE 1815 (DNP3) being common in North America, IEC 61850 internationally focused, and DLMS/COMSEM serving as the standard in European countries. These protocols incorporate various security measures, including authentication (referred to as security level) and encryption (referred to as security suite) (Butun et al., 2020). Both authentication and encryption often make use of the same security keys, which can be independently chosen or used in combination. The selection of cryptographic algorithms heavily depends on the vendor, with options such as MD5, SHA1, SHA256, GMAC, and ECDSA being available. Subsequently, the chosen key is utilized as an encryption measure for individual messages within the grid. For instance, DLMS/COMSEM relies on the AES128 with GCM operation mode enabled cryptographic algorithm for this purpose (Butun et al., 2020).

3.6. Other Attack Types

The smart grid infrastructure is a complex system that integrates various technologies to provide efficient and reliable energy distribution. However, this infrastructure is vulnerable to various types of attacks, including but not limited to denial of service, radio signal jamming, replay, and identity, which can result in electric or data loss, disruption of normal function (also known as "bricking"), and erosion of consumer trust (Butun et al., 2020).In addition to the smart grid infrastructure, smart cities offer services across six domains, including smart grids, renewable energy, parking control, 3D city models, and citizen participation platforms. These services are designed to increase quality of life and enhance sustainability of municipal environments. However, the focus of these services varies by region, with European cities emphasizing energy, resources, and democracy, Asian cities prioritizing public transportation and disaster mitigation, and American cities concentrating on crime prevention (Yang, 2021).

Despite the data-driven nature of these domains, there is limited discussion regarding data security (transit or storage) and privacy. This is a significant concern, as the collection and analysis of data from these domains can reveal sensitive information about individuals and communities. For example, data from smart grids can reveal patterns of energy consumption, which can be used to infer the behavior and lifestyle of individuals. Similarly, data from citizen participation platforms can reveal the opinions and preferences of individuals, which can be used to influence political decisions (Sookhak et al., 2018). To address these concerns, it is essential to implement robust data security and privacy measures that protect the confidentiality, integrity, and availability of data. This includes the use of encryption, access controls, and secure communication protocols to ensure that data is transmitted and stored securely. Additionally, it is crucial to establish clear policies and guidelines for data collection, use, and sharing to ensure that individuals' privacy rights are respected (Sookhak et al., 2018).

4. Let's talk about privacy

To begin to address consumer concerns, Kamil and Ogundoyin (2018) examined the use of a lightweight fault tolerant pricy data aggregation scheme leveraging elliptic curve cryptography and hashing chain. Understanding security protocols for smart grids, smart cities, and smart technology is necessary to implement and secure smart technology to protect consumer privacy. As smart technology is deployed at a faster pace than regulation can keep up with as well as identifying vulnerabilities within smart technology; it becomes necessary to better understand what smart technology is currently available.

4.1. Examples of Smart Cities around the world (and their privacy laws)

The existing literature outlines the best practices and security requirements for smart cities. However, it is evident that the current security measures are inadequate for the unique challenges posed by smart cities. Despite the implementation of these security requirements, companies continue to experience data breaches daily, often due to factors such as human error and delays in system patching. In the event of an attack or breach, the current recommendations include identity theft monitoring, registration on "do not call" lists, system patching and updates, secure booting, and lifecycle management for systems, applications, and solutions (Sookhak, et. al., 2018). Given these limitations, there is an urgent need for innovative and more effective approaches to securing smart cities at the local and individual levels to mitigate the risks to consumer privacy. While it is acknowledged that some level of risk will always be present, it is imperative for governments, companies, and users to collaborate to transparently manage and communicate these risks. This entails ensuring that comprehensive knowledge regarding the risks associated with smart cities is readily available to all stakeholders.

To facilitate this process, having knowledge of privacy laws that are in effect in countries where smart cities are being developed. By examining the privacy laws of these countries, we can gain insights into the legal framework governing data protection and privacy within smart cities. This knowledge is essential for developing robust security measures that align with the regulatory requirements of each country. The inadequacy of current security requirements for smart cities necessitates a paradigm shift towards more effective and tailored approaches to address the unique privacy and security challenges they present. By understanding and adhering to the privacy laws of countries with smart cities, stakeholders can proactively enhance the security posture of these urban environments while safeguarding the privacy rights of their inhabitants.

4.2. Singapore

Singapore has been recognized as a leading smart city, ranking 10th in 2019 and 7th in 2023 according to the IMD Smart City index report (IMD Smart city, 2022). This achievement is attributed to Singapore's use of technology to improve its urban areas, making its citizens healthier and its city more sustainable (Bris, 2019; Sivaramakrishnan, 2019). The implementation of smart parking, intelligence transport system, waste and water management,

and behavioral monitoring are some of the key initiatives that have contributed to Singapore's smart city status (Green, 2016).

Smart parking is a technology enabling drivers to trace vacant parking spaces in real-time, decreasing the search time for parking spots and minimizing traffic congestion (Green, 2016). The intelligence transport system utilizes enhanced data analytics and real-time data gathering procedures to boost traffic flow, reduce travel time, and improve road safety (Sivaramakrishnan, 2019). Waste and water management initiatives involve the use of sensors and data analytics to monitor and manage waste and water resources, reducing waste and conserving water (Sivaramakrishnan, 2019). Behavioral monitoring is a technology that uses sensors and data analytics to track human behavior, enabling city planners to design more efficient and sustainable urban areas.

However, with the increasing use of technology in governing and monitoring urban areas, it is important to review privacy laws to ensure that personal data is protected. Singapore's personal data protection act (PDPA) is a regulation covering the collection, use, disclosure, and care (Personal Data Protection Commission, n.d.). The PDPA defines personal data as any data which is to be used for personal identification, including name, address, and contact details. The regulation necessitates any organization to acquire clear consent from any impacted individual prior to the collection of any personal data, and to safeguard the data being used only for the purpose the data was collected. Additionally, PDPA includes a provision requiring organizations to undertake reasonable protection steps for the data aiding to eliminate unauthorized access, disclosure, or misuse (Personal Data Protection Commission, n.d.). Singapore's smart city initiatives have been successful in improving its urban areas and making its citizens healthier. However, it is important to ensure that personal data is protected in the process. The PDPA includes a framework for the collection, use, and protection of personal data, ensuring that individuals' privacy rights are respected.

4.3. United States

The implementation of comprehensive privacy laws in the United States is a significant step towards protecting consumers' personal data. The seven states that have enacted such laws, including California, Colorado, Connecticut, Utah, Iowa, Virginia, and Rhode Island, have put in place measures to regulate the collection, usage, and sharing of personal information (Desai, 2023).

The Virginia’s Consumer Data Protection Act and California Consumer Privacy Act (CCPA) are examples of state driven privacy laws that provide individuals with greater control over their personal data. State laws grant consumers the right to access, delete, and control the sale of any personal data. CCPA, requires organizations to disclose the categories of personal data collected, the purpose of collection and use, and any third parties with whom the data will be shared (State of California Department of Justice, 2023).

The privacy laws in Colorado, Connecticut, and Utah, which are set to take effect soon, also aim to empower consumers and impose obligations on businesses to ensure the responsible

handling of personal data. The Colorado Privacy Act (CPA) has a provision enabling consumers the right to opt-out of any sale of, access to, correction of inaccurate data, and to request the deletion of personal data (Desai, 2023; n.a., 2023). The CPA also requires businesses to conduct data protection assessments and implement reasonable security measures to protect personal data (State of Connecticut, 2022). Moreover, the need for transparent privacy laws in smart cities is becoming increasingly important. Many cities, such as Dallas, Chicago, and San Francisco, are not located in states with comprehensive privacy laws (Lively, 2022; McNamara, 2023). This highlights the need for smart cities to have transparent privacy laws in place to safeguard personal data and limit the risk of misuse. The implementation of comprehensive privacy laws in the United States is a crucial step towards protecting consumers' personal data (Locke, 2020). These laws provide individuals with greater control of personal data and levy duties on organizations ensuring the responsible handling of personal data. The need for transparent privacy laws in smart cities is also emphasized, highlighting the importance of safeguarding personal data, and minimizing potential misuse.

4.4. China

This article provides valuable insights into China's Smart City project and its data-driven strategy. One of the key takeaways is that smart city data in China is often owned by the government or industry, and the lack of interoperability between databases can hinder effective data sharing for predictive analysis. This has resulted in a default "control room" design for smart city operations, which has limited predictive capabilities and often leads to a reactive mode of operation (Chen et al., 2016).

To address these challenges, the China Smart City project has focused on three pillars: cycle-data collection, analysis, and data-driven smart services (Chen et al., 2016). These pillars are essential for the development of new smart cities and have been driven by two distinct groups of users: citizens and data scientists. The participation of citizens during the development of smart cities is fundamental as they are the end-users and can provide valuable feedback on the effectiveness of the services provided. Data scientists, on the other hand, play a critical role in analyzing the vast amounts of data generated by smart cities and developing predictive models to improve city operations. However, the development of smart cities in China has not been without its challenges. One of the main issues is the lack of interoperability between databases, which can hinder effective data sharing and analysis. Additionally, there are potential privacy and security concerns related to the data collection and use within smart cities. To address these concerns, China has passed several data privacy and security laws, including the Cybersecurity Law of the People's Republic of China (CSL) in 2017, the Personal Information Protection Law of the People's Republic of China (PIPL) in 2021, and the Data Security Law (DSL) in 2021. These laws aim to regulate the gathering, use, and safeguard of personal information in smart cities and ensure that citizens' privacy rights are respected (Privacy Research Team, 2021). While there are challenges associated with the development of smart cities in China, the focus on data-driven smart services and the involvement of citizens and data scientists are promising steps towards creating more efficient and sustainable cities.

4.5. Surakarta City, Indonesia

The World Bank's projection for 2045 indicates a significant shift, with an estimated 75% of Indonesia's population, roughly 220 million people, expected to be residing in urban areas. In response to this impending urbanization, the Indonesian government has embarked on a proactive endeavor to address the multifaceted implications through the implementation of a comprehensive smart city strategy. This strategy encompasses the intricate design of multi-dimensional clusters, integrating three fundamental dimensions: People, which encompasses intelligence, inventiveness, and creativity; Collective Intelligence, focusing on knowledge and innovation; and Artificial Intelligence, encompassing infrastructure and communications. The overarching goal of this strategic initiative is to cultivate a culture of innovation rooted in smart technology concepts. A recent study has meticulously identified 55 innovations, among which 16 have been earmarked as government priorities, forming the cornerstone of the quick-win strategy for Smart City development (Nugroho et al., 2022).

4.6. Brazil

The development of the Maturity Model for Smart and Sustainable Cities in Brazil (MMSSCB), which was created based on the recommendations of the International Telecommunication Union (ITU). The ITU had previously developed a maturity model for sustainable smart cities, which was tested in Brazil. However, it was found that the ITU model was not viable for implementation in an emerging country like Brazil. The ITU model consisted of seven levels: Accession, Commitment, Planning, Alignment, Development, Integration, and Optimization. However, the new MMSSCB model was designed to be more suitable for the Brazilian context. The MMSSCB model aims to foster public policies and has been designed to be implemented in all 5570 cities in Brazil (Loureiro et al., 2021).

The MMSSCB model is expected to have significant implications for Brazilian cities. By using this model, cities can assess their current level of development in terms of smart and sustainable practices. This assessment can help cities identify areas for improvement and prioritize actions to achieve their sustainability goals. Additionally, the model can aid policymakers to advance more effective policies and strategies promoting sustainable development in Brazilian cities (Loureiro et al., 2021). Overall, the MMSSCB model has the potential to contribute to the creation of more livable, resilient, and sustainable cities in Brazil.

4.7. Nigeria

This article provides valuable information about the development of smart cities in Nigeria, particularly in Port-Harcourt. One of the key projects discussed is Silicon Delta, which is being developed by bamboo Real Estate and Construction Limited. The project aims to address the shortage of quality and conducive accommodation in Nigeria, which has led to many people leaving the country. Silicon Delta is envisioned as a smart green city where creative minds can live, work, play, and create. The project is expected to be completed by 2030 (Lukhanyu, 2022).

Another smart city being promoted in Nigeria is Eko Atlantic City. Both Silicon Delta and Eko Atlantic City are expected to leverage technology and innovation to create sustainable and livable urban environments (Baraka, 2021). However, as these cities collect and process large amounts of data, it is important to ensure that citizens' privacy is protected.

The legal framework for data protection in Nigeria. Section 37 of Nigeria's constitution guarantees citizens' right to privacy, and the Data Protection Regulation 2019 (NDPR) provides further protection for personal data (Ekweozor, 2020). The NDPR states personal information is any data which relates to an identified individual to identify them directly or indirectly. This includes data such as name, location, online identifiers, genetic and mental health information, and email addresses. Companies and entities that store personal data in Nigeria are responsible for protecting this data and ensuring compliance with the NDPR. Nigeria’s promotion of smart cities and importance of protecting citizen privacy in the process, highlights the legal framework for data protection in Nigeria and the types of personal data that are protected under the NDPR (Roberts et al., 2021).

4.8. Kenya

The Data Protection Act, 2019 (DPA) in Kenya plays a crucial role in regulating the collection, handling, and transfer of individuals' information, thereby safeguarding their fundamental right to privacy (Githaiga et al., 2023). This legislation is significant as it outlines specific provisions aimed at ensuring the responsible and ethical use of personal data. For instance, it may include guidelines on obtaining consent for data collection, ensuring data security, and establishing individuals' rights to access and control their personal information. Furthermore, the Kenya Open Data Initiative, spearheaded by the Nairobi City County and the Ministry of Transport and Infrastructure, aims to revolutionize city planning and citizen engagement by collecting transportation data (Klopp, 2016). This initiative holds the potential to enhance urban development and improve the overall quality of life for citizens. By leveraging transportation data, city planners can make informed decisions to address traffic congestion, optimize public transportation systems, and create more sustainable urban environments. Additionally, citizens can benefit from access to real-time transportation information, leading to improved commuting experiences and enhanced mobility.

The Konza smart city project represents a significant endeavor in Kenya, with a focus on integrating advanced technologies to create a modern urban center (Baraka, 2021). The project's infrastructure, including its own data center, disaster recovery center, optical fiber network, and IoT infrastructure, underscores the ambition to build a technologically advanced and interconnected city (Chepkemoi, 2023). However, the prolonged construction period of 13 years raises questions about the project's completion and the need for further research on data management and utilization once the city becomes operational. Addressing these challenges is crucial to ensure the seamless integration of data-driven technologies and the effective functioning of the smart city (Chepkemoi, 2023).

The DPA, the Kenya Open Data Initiative, and the Konza smart city project collectively represent significant developments in Kenya's data protection and urban development

landscape. These initiatives underscore the country's commitment to leveraging data responsibly for the benefit of its citizens while also highlighting the need for ongoing research and strategic planning to address the complexities associated with data management in the context of smart city development.

4.9. South Africa

Cape Town, the capital of Western Cape, boasts a diverse economy driven by manufacturing, tourism, finance, logistics, and information technology. Cape Town's government has embarked on a comprehensive four-pillar initiative aimed at achieving smart city status. These pillars include the development of digital infrastructure, e-government, and economy (Veras, 2017). Within the context of privacy, South Africa's constitution, ratified in 1996, enshrines the right to privacy in section 14. This constitutional provision mandates the protection of the bill of rights and the privacy of citizens, encompassing the privacy of their communications. However, it's important to note that constitutional protection does not explicitly cover digital privacy, excluding certain areas such as health records (n.a., 2019).

5. Misuse cases and Risks of potential misuse

Delving into the crucial need for multiple perspectives when developing AI, smart cities, and other algorithmic software. The potential for biased data sets to be used, as there is often only one learning tool. This can lead to significant issues, such as discrimination and misidentification, particularly when it comes to facial recognition technology. To address these concerns, the development phase must prioritize security and privacy measures and undergo a rigorous multi-layered quality control process before the release and implementation of AI software and smart cities. This is essential to prevent misuse cases, such as the exploitation of weaknesses in IoT devices or the use of surveillance technology to obtain information on political rivals.

Robin Pocorie, a graduate student, from the Dutch University VU Amsterdam was trying to take an online exam; however, the mandatory facial recognition software for online exams, would not recognize her (Meaker, 2023). The software was created by Proctorio and purchased by the university to prevent students from cheating. Pocornie is black and when she attempted to take her exam the software returned an error stating "no face found" until she used a lamp (extremely close to her face) to highlight her facial features (Meaker, 2023). Pocornie is currently challenging the university's use of the facial recognition software as it discriminates against black students, and they are forced create complex lighting effects just to take exams (Meaker, 2023). Unfortunately, Pocorie's experience is not unusual. According to Raji (2019), audited commercial face-recognition products and found the products were 30% worse at identifying dark skinned women (Raji, 2019) This approach must prioritize security, privacy, and unbiased data sets to prevent discrimination and misuse cases and ensure that these technologies benefit all citizens.

These cases highlight the potential for discrimination and misidentification, particularly when it comes to facial recognition technology. One example cited is the case of Madison Square Garden (MSG) entertainment, which uses facial recognition in their event centers and buildings. A woman was removed from a Roquettes event because she worked for a law firm that was suing the MSG company (McShane, 2022). Despite not being involved in the case against MSG, she was not allowed entry due to the facial recognition software used for the safety of their customers (McShane, 2022).

Delving into the intricate intersection of technology, security, and human rights, shedding light on the potential misuse of surveillance technology by both private entities and governments. It specifically highlights the activities of Circles, a surveillance firm that offers products capable of exploiting vulnerabilities in telecommunications architecture to intercept communications and track individuals globally. The report identifies several countries as likely customers of Circles, some of which have a troubling history of human rights violations and a documented pattern of using surveillance technology against their own citizens (Dave, 2020). Furthermore, the document discusses a notable incident involving the misidentification of an individual by the Detroit police department, which relied on facial recognition technology. This case underscores the ethical and accurate concerns associated with the use of such tools by law enforcement agencies. It emphasizes the need for robust safeguards and ethical guidelines to prevent wrongful arrests and protect individual rights in the context of evolving surveillance technologies (Fruhlinger, 2018).

In addition, we explore the security vulnerabilities in IoT devices, exemplified by the Mirai botnet, which exploited weaknesses in IoT devices, such as CCTV cameras, through default passwords and inadequate security configurations (Fruhlinger, 2018). This example underscores the urgent need for enhanced security measures in IoT devices, especially as smart cities and interconnected devices become more prevalent. It emphasizes the imperative of implementing stringent security protocols and eliminating default insecure settings in IoT devices to mitigate the risks associated with potential cyberattacks and unauthorized access (Hernandez-Ramos et al., 2021). A comprehensive analysis of the ethical, security, and human rights implications of emerging technologies, urging stakeholders to address these multifaceted issues to ensure a safer, more responsible, and rights-respecting technological landscape.

The Citizen lab, out of Toronto, published a report on the company Circles, which is a surveillance firm selling to countries around the world. The report from Marczak et al., (2020) out of the Citizen Lab Research report, found Circles is a surveillance firm that sell products which can “exploit weaknesses” within the telecommunications architecture to eavesdrop on phone calls, text messages and gather the locations of phones around the world (p.1). The report notes Circles is linked with NSO Group, who develops Pegasus spyware (Marczak et al., 2020). Marczak et al. (2020) conducted scans via the Internet and found “unique signatures” linked to firewall hostnames deployed by Circles (p1). The following countries were likely customers of Circles as determined by the Citizen Lab:

Australia, Belgium, Botswana, Chile, Denmark, Ecuador, El Salvador, Estonia,

Equatorial Guinea, Guatemala, Honduras, Indonesia, Israel, Kenya, Malaysia, Mexico,

Morocco, Nigeria, Peru, Serbia, Thailand, the United Arab Emirates, Vietnam, Zambia, and Zimbabwe.

The Circles' firm and products use the Signaling System 7 (SS7) protocol suite, which handles "roaming in 2G and 3G mobile networks" (Marczack et al., 2020, p.2). The SS7 protocol was developed in 1975 and did not include any sort of authentication, thus allowing anyone to send commands to a customer's network and track their location and intercept text messages (Marczack et al., 2020). Some countries identified in the report had a history of human rights violations and a track record of using surveillance technology against their citizens.

On the topic of surveillance technology, there are several examples of countries that have misused this technology to suppress dissent and curtail freedom of speech. For instance, Botswana used surveillance technology to prevent citizens from reporting government corruption, while Chile intercepted messages from journalists and Indigenous Mapuche leaders to justify arrests (Marczack et al., 2020). In Nigeria, the government reportedly used surveillance technology to obtain information on political rivals. These are just a few of the 25 countries discussed in the report (Marczack et al., 2020).

The document also raises concerns about the development and use of AI systems like ChatGPT. OpenAI's ChatGPT, for example, was trained by scraping millions of web pages, books, and posts, as well as some personal information, which violates EU privacy laws or GDPR rules (Burgess, 2023). Italy demanded that OpenAI stop using personal information on Italian citizens in its training data as it is illegal. Additionally, there have been concerns raised by artists who claim that AI developers were using their work without permission (Burgess, 2023). As a result, there has been a call to halt the development and use of ChatGPT and other AI systems until further research can be done (Burgess, 2023). Also emphasizing the importance of unbiased data sets and the inclusion of all perspectives, particularly when it comes to facial recognition technology. Dr. Buolamwini and Dr. Timnit Gebru's study on "Gender Shades" highlights the need for all people, from white to black and all shades of black and brown, to be included in facial recognition datasets (Buolamwini & Gebru, 2018). Our research stresses the need for responsible and transparent use of surveillance technology in smart cities. Without proper regulations in place, the misuse of surveillance technology will continue and potentially increase, resulting in a reduction of quality of life for people and causing more harm.

6. Future Research and Recommendations

The rapid expansion of smart cities has led to the extensive collection of citizen data through various connected services. This has raised significant concerns regarding consumer privacy and security. The article emphasizes the pressing need for comprehensive research to address these concerns and maintain consumer privacy in the evolving landscape of smart cities. One crucial area highlighted in the document is the necessity for research on the effectiveness of consumer security and privacy requirements surrounding data protections. This includes the identification of successful implementations of securing citizen data within smart cities and technology. Moreover, the article underscores the importance of integrating security and

privacy goals and objectives at the core of smart city designs. It calls for the identification of standards that offer flexibility in response to shifting privacy and security laws and policies.

Furthermore, the article emphasizes the need to balance public safety with citizen privacy, particularly in the context of surveillance technologies. It advocates for the establishment of a smart city data sharing clearinghouse to consolidate best practices and lessons learned, promoting fair and ethical use of public safety data. In anticipation of impending regulations surrounding privacy acts, stressing the requirement for greater transparency in data collection and usage by organizations. It also highlights the gap in addressing automated decision making and the use of artificial intelligence within smart technology, signaling the need for future research to outline risks to consumers and guide governmental measures to ensure secure data collection and utilization within smart cities. Overall, this underscores the responsibility of smart cities in protecting the data collected from citizens to deliver essential services. It also references the European data protection law as an example of the legal framework that smart cities must adhere to, emphasizing the global relevance of these privacy and security considerations (Vandercruysse et al., 2022).

7. Conclusion

Smart cities are a complex system that requires real-time monitoring, inter-connected multiple systems, and the collection of vast amounts of data from devices and citizens. Researchers have discussed the definition and functionality of smart cities, as well as the privacy laws that exist in different countries. They have also highlighted the potential misuse of AI and surveillance technology, which can cause harm to individuals. Therefore, it is crucial to prioritize security and privacy when developing smart cities to limit harm to people.

The literature gap indicates the need for further research on the technical aspects of smart city deployments and their impact on society. For instance, it is essential to investigate whether smart cities deliver on their promises and improve citizens' lives. Additionally, prioritizing consumer privacy and security should be a primary consideration from the outset of implementing smart city and smart grid technology. According to Sookhak et al. (2018), many smart cities are not efficient in safeguarding of security and privacy due to the collection, storage, and real-time analysis of vast amounts of data. Therefore, it is crucial to determine who is responsible when a data breach occurs and when a person's loss of data privacy has tangible consequences. In summary, this article emphasizes the importance of privacy and security in smart cities. By prioritizing these factors, we can ensure that smart cities deliver on their promises and improve the lives of citizens.

Acknowledgement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1. Baraka, C. (June 2021). The failed promise of Kenya's smart city. https://restofworld.org/2021/the-failed-promise-of-kenyas-smart-city/
2. Barkan, E., Biham, E., & Keller, N. (2003). Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. In: Boneh, D. (eds) Advances in Cryptology - CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol 2729. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45146-4_35
3. Barkan, E., Biham, E., and Keller, N. (2008). Instant ciphertext-only cryptanalysis of gsm encrypted communication. *Journal of Cryptology, 21*(3), 392–429. https://doi.org/10.1007/s00145-007-9001-y
4. Boehme-Neßler, V. (2016). Privacy: A matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law, 6*(3), 222–229. https://doi.org/10.1093/idpl/ipw007
5. Bris, A. (October 2019). Smart cities: world's best don't just adopt new technology, they make it work for people. https://www.weforum.org/agenda/2019/10/smart-cities-world-s-best- don-t-just-adopt-new-technology-they-make-it-work-for-people
6. Burgess, M. (April 2023). ChatGPT has a big privacy problem. https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/
7. Butun, I., Lekidis, A., & dos Santos, D. (2020). *Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities* [paper presentation]. 6th International Conference on Information Systems Security and Privacy - ICISSP, Valletta, Malta. http://dx.doi.org/10.5220/0009187307330741
8. Boisvert, N. (2020). LGBTQ activist Sarah Hegazi, exiled in Canada after torture in Egypt, dead at 30. https://www.cbc.ca/news/canada/toronto/sarah-hegazi-death-1.5614698
9. Chen, C., Wang z., and Guo B. (2016). "The Road to the Chinese Smart City: Progress, Challenges, and Future Directions," *IT Professional, 18*(1), 14-17. doi:10.1109/MITP.2016.2.
10. Chepkemoi, C. (March 2023). Setting the sails right-the making of a smart city "Konza technopolis". https://www.edgelands.institute/blog/setting-the-sails-right-the-making-of-a-smart-city-konza-technopolis
11. Code of Virginia, (n.d.). Data controller responsibilities; transparency. https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/
12. Crosston, M. *(2020).* Cyber colonization: The dangerous fusion of artificial intelligence. *Cyber, Intelligence, and Security, 4(1).* https://www.inss.org.il/publication/cyber-colonization-the-dangerous-fusion-of-artificial-intelligenceand-authoritarian-regimes/
13. Denai, A. (2023). US State comprehensive privacy laws report-overview. https://iapp.org/resources/article/us-state-privacy-laws-overview/
14. Denai, A. (2023). Iowa becomes sixth US state to enact comprehensive consumer privacy legislation. https://iapp.org/news/a/iowa-becomes-sixth-us-state-to-enact-comprehensive-consumer-privacy-legislation/
15. Döbelt, S., Jung, M., Buscha, M., & Tscheligi, M. (2015). Consumers' privacy concerns and implications for a privacy preserving smart grid architecture—Results of an austrian

study. *Energy Research & Social Science,* 9, 137-145. http://dx.doi.org/10.1016/j.erss.2015.08.022

16. Ekweozor, E. (2020). An Analysis of the Data Privacy and Protection Laws in Nigeria. *SSRN*. http://dx.doi.org/10.2139/ssrn.3639129
17. Githaiga, J. & Kurji, J. (February, 2023). Kenya: Data privacy comparative guide. https://www.mondaq.com/privacy/1190020/data-privacy-comparative-guide
18. Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. A. (2022, November 29). NIST framework and Roadmap for Smart Grid Interoperability Standards, release 4.0. NIST. https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40
19. Green, J. (2016). The smart city playbook: Smart, safe, sustainable. https://onestore.nokia.com/asset/200700
20. Founoun A. & Hayar, A. (2018). "Smart City concept's energy awareness assessment through sustainable development standards," *2018 Renewable Energies, Power Systems & Green Inclusive Economy (REPS-GIE)*, Casablanca, Morocco, 1-6, doi:10.1109/REPSGIE.2018.8488808.
21. Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

22. Kamil, I. A., & Ogundoyin, S. O. (2018). EPDAS: Efficient privacy-preserving data analysis scheme for smart grid network. *Journal of King Saud University-Computer and Information Sciences, 33*(2), 208-217. https://doi.org/10.1016/j.ksuci.2018.12.009

23. Kebotogetse, O., Samikannu, R. & Yahya, A. (2021). Review of key management techniques for advanced metering infrastructure. *International Journal of Distributed Sensor Networks, 17*(8). https://doi.org/10.1177/15501477211041541

24. Kessel, P., & Glavitsch, M. (1986). Estimating the Voltage Stability of a Power System. *IEEE Transactions on Power Delivery, 1*(3), 346-354. https://doi.org/10.1109/TPWRD.1986.4308013
25. Kistler, R., Bieri, M., Wettstein, R., & Klapproth, A. (2009). *Tunneling smart energy protocols over zigbee* [paper presentation]. 14th IEEE International Conference on Emerging Technologies & Factory Automation. Palma de Mallorca, Spain. https://dl.acm.org/doi/10.5555/1740954.1741124
26. Kumari, A., & Tanwar, S. (2020). Secure data analytics for smart grid systems in a sustainable smart city: Challenges, solutions, and future directions. *Sustainable Computing: Informatics and Systems, 28*, 100427. https://doi.org/10.1016/j.suscom.2020.100427
27. L. C. Loureiro, C. Muniz, C. Pereira, L. Paseto, M. Martinez and A. M. Alves, "A new methodology for smart cities in developing countries: a case study," *2021 IEEE International Smart Cities Conference (ISC2)*, Manchester, United Kingdom, 2021, pp. 1-6, doi:10.1109/ISC253183.2021.9562923.
28. Lively, T. (Mar 2022). Utah becomes fourth US state to enact comprehensive consumer privacy legislation. https://iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/

29. Locke, J. (October 2020). Top 12 smart cities in the U.S. -Smart cities examples 2020. https://www.digi.com/blog/post/smart-cities-in-the-us-examples
30. Lukhanyu, M. (May 2022). Nigeria's bamboo to develop first smart city, Silicon Delta, in Port-Harcourt. https://techmoran.com/2022/06/06/nigerias-bamboo-to-develop-first-smartcity-silicon-delta-in-port-harcourt/
31. Marczak, B., Scott-Railton, J., Prakash Rao, S., Anstis, S. & Deibert, R., (2020). Running in Circles- Uncovering the clients of cyberespionage firm Circles. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm- circles/.
32. Mardacany, E. (2014). "Smart cities characteristics: importance of built environments components," *IET Conference on Future Intelligent Cities*, London, pp. 1-6, doi:10.1049/ic.2014.0045.
33. McNamara, J. (February 2023). *H5745- Rhode Island personal data and online privacy protection act.* https://status.rilegislature.gov/
34. McShane, J. (December 2022) Girl Scout mom kicked out of Radio City and barred from seeing Rockettes after facial recognition tech identified her. https://www.nbcnews.com/news/us-news/girl-scout-mom-kicked-radio-city-barred-seeing-rockettes-facial-recogn-rcna62606
35. Meaker, M. (April, 2023). This student is taking on 'biased' exam software. https://www.wired.com/story/student-exam-software-bias=proctorio/#:~:text=Mandatory%20face%2Drecognition%20tools%20have,fighting%20to%20end%20their%20use.
36. n.a., (March, 2023). Attorney General's office files finalized Colorado Privacy Act rules https://coag.gov/press-releases/3-15-23/
37. n.a., (January 2019). State of privacy South Africa. https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa
38. Nugroho, R., Prakoso, S., Hidayati, K., Rahmawati, A. (2022). "Smart Technology Maturity and Smart City Initiative: Is it inline? A case in Surakarta City," *2022 1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS)*, Surakarta, Indonesia, 2022, pp. 75-78, doi: 10.1109/APICS56469.2022.9918743.
39. Roberts, T., Mohamed Ali, A., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). *Surveillance law in Africa: A review of six countries*, Brighton: Institute of Development Studies. DOI: 10.19088/IDS.2021.059
40. Personal Data Protection Commission, (n.d.) PDPA overview. https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
41. Pillitteri, V. Y., & Brewer, T. L. (2014). *Guidelines for Smart Grid Cybersecurity* (Report No. 7628). National Institute of Standards and Technology. https://dx.doi.org/10.6028/NIST.IR.7628r1
42. Privacy research team (2021, September). Overview of Personal Information Protection Law of the People's Republic of China. https://securiti.ai/china-personal-information-protection- law-overview/
43. Richards, N. (2021). *Why privacy matters.* Oxford University Press.
44. Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.

45. Sharifi A, Allam Z, Feizizadeh B, Ghamari H. (2021). Three decades of research on smart cities: Mapping knowledge structure and trends. *Sustainability. 13*(13):7140. https://doi.org/10.3390/su13137140
46. Sivaramakrishnan, S. (November 2019). 3 reasons why Singapore is the smartest city in the world. https://www.weforum.org/agenda/2019/11/singapore-smart-city/
47. Sookhak, M. Tang, H., He, Y., & Yu, R. (2018) Security and privacy of smart cities: A Survey, research issues and challenges. *IEEE Communications Surveys & Tutorials, 21*(2), 1-26. doi:10.1109/COMST.2018.2867288
48. Solove, D. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law*, 44(4), 745-772. https://digital.sandiego.edu/sdlr/vol44/iss4/5
49. State of California Department of Justice. (May 2023). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa
50. State of Connecticut, (June 2022). Governor Lamont signs legislation enacting a comprehensive consumer data privacy law. https://portal.ct.gov/Office-of-the-Governor/News/Press-Releases/2022/06-2022/Governor-Lamont-Signs-Legislation-Enacting-a-Comprehensive-Consumer-Data-Privacy-Law
51. Strittmatter, K. (2020). We Have Been Harmonized: Life in China's Surveillance State.
52. HarperCollins.
53. Stilinovic, M. and Hutchinson, J. (2022), The Internet regulation turn? Policy, Internet and technology. Policy Internet, 14: 6-12. https://doi.org/10.3390/s22051838
54. Vandercruysse, L., Christofi, A., Buts, C., Dooms, M., & Valcke, P. (2022). Data Protection in Smart Cities: Pre-Commercial Procurement as a Silver Bullet? *European Procurement & Public Private Partnership Law Review*, *17*(2), 81–93. https://doi-org.captechu.idm.oclc.org/10.21552/epppl/2022/2/5
55. Veras T, (10 April 2017). Smart cities in Africa: Nairobi and Cape Town.
56. Yang, J., Kwon Y., and Kim, D. (2021). "Regional Smart City Development Focus: The South Korean National Strategic Smart City Program," in *IEEE Access*, 9, 7193-7210. doi:10.1109/ACCESS.2020.3047139.
57. Zhang, H., Liu, B., & Wu, H. (2021). Smart Grid Cyber-Physical Attack and Defense: A Review. *IEEE Access, 9*, 29641-29659. https://doi.org/10.1109/access.2021.3058628