**LITERATURE SURVEY**

The literature has tended to focus on a number of broad smart cities related key themes namely: The privacy and security of mobile devices and services; smart cities infrastructure and technical architecture; power systems utilized within smart cities; smart healthcare; security and privacy frameworks; algorithms and protocols; operational threats for smart cities; application of blockchain solutions within smart cities; and social media and smart cities. The below Figure presents the research themes and the percentage of papers grouped under each theme. The themes and related references are listed in below Table. The subsections of the article generated discussion around each theme providing insights to research carried under the respective main themes.

**1) Privacy and Security of Mobile Devices and Services:**

Mobile devices are the backbone of interacting with the smart cities network infrastructure but present new challenges to the security and privacy of users where sensitive data could be vulnerable to attack by third parties. The study presented three novel approaches for satisfying the required privacy of mobile devices within smart cities. The first approach utilized the concept of foggy dummies to protect the privacy of the user; the second incorporated a blind third party where a trust relationship is developed to protect the user from the server provider; the third approach used the concept of a double foggy cache to solve the trust issue between peers with a traditional cooperation approach. Privacy-preserving authentication (PPA) protocols for mobile services have emerged as a promising cryptographic approach to provide authentication and privacy protection features for smart cities. The research presented in Li et al. (2019) analyzed the PPA protocol suitability for mobile services within a typical mobile service application in a smart city context.

**2) Smart City Infrastructure:**

A number of articles focused on smart city infrastructure and ways to overcome security and privacy issues within smart cities (Abosaq 2019; Ainane et al. 2018; Alandjani 2018; Antoine Picon 2019; Awad et al. 2019; Baryshev et al. 2016; Bernardes et al. 2018; Chatterjee et al. 2017; de Amorim et al. 2019). Studies have argued that privacy can be easily compromised due to the high levels of interaction between people, devices and sensors, thus highlighting the need for this data to be fully protected (Antoine Picon 2019; Elmaghraby and Losavio 2014). Studies have posited the merits of a more strategic focus on smart city security looking beyond aspects of data privacy toward a smart securitisation policy (Efthymiopoulos 2015).

The study by Ferraz and Ferraz (2014a) argued that information security does not only include privacy, confidentiality, integrity and availability, but also includes interoperable security that represents the idea of a general failure of the urban system.

**3) Smart Power System:**

The power system aspects of smart cities are of critical importance within the overall security and privacy infrastructure, as third parties connected to the grid could monitor usage patterns and predict consumers’ behaviour. The wireless network technology focused nature of the many systems that supply and control heat and light to smart cities, could expose the grid to security vulnerabilities. Alamaniotis et al. (2017) presented an intelligent methodology for enhancing privacy within smart power systems. The proposed methodology utilized demand patterns for several consumers connected to the power grid to provide a new consumption pattern. The study by Sanduleac et al. (2016) addressed two main aspects of smart city implementation; namely: (i) multi-energy streams when different utilities serve different energy networks in the city such as electricity, gas, and heat (ii) the issue of engaging the citizens by sharing their private energy data profile, as an alternative to implementations that fail to progress from small pilots to large deployment.

**4) Smart Healthcare:**

The security and privacy of healthcare services and concepts within smart cities are a key factor in the overall minimal disclosure of data and information security infrastructure (Maria De Fuentes et al. 2018). The research by Alromaihi et al. (2018) identified the main security and privacy challenges in designing IoT architecture in the context of healthcare applications, highlighting the increased use of sensors for medicine and healthcare applications over the last decade. The study identified key threats from personal health related data captured via sensors for e.g. heart rate and also blood pressure and the importance of an integrated security solution for the entire system.

**5) Frameworks, Models, Algorithms and Protocols to Improve Security and Privacy:**

As smart cities face a number of challenges connected to security and privacy, some studies proposed various frameworks, models and algorithms to improve these issues (Al-Dhubhani et al. 2018; Antonopoulos et al. 2017; Avgerou et al. 2016; Beltran et al. 2017; Burange and Misalkar 2015; Cagliero et al. 2015). This aspect of the literature has focused on encryption algorithms to build in security to smart city systems. The Antonopoulos et al. (2017) study tests high-level security feature algorithms by using Wireless Sensor Network (WSN) development. Stromire and Potoczny-Jones (2018) proposed to integrate an end-to-end cryptography system into smart city solutions at a foundation level. During any data breach, nothing about the data would be revealed by applying this system.

**6) Operational Vulnerabilities for Smart Cities:**

Data within smart city applications should be able to withstand modification, disruption, inspection, unauthorised access, disclosure and annihilation. Basic requirements for security and privacy include confidentiality, integrity, availability, nonrepudiation, access control and privacy (Dewi Rosadi et al. 2018). Privacy is a core issue within smart cities and one that can be directly linked to the minimal understanding of privacy from local government and business in the way they collect and process personal data. Often they do not provide the community with the opportunity and mechanism for consent (Dewi Rosadi et al. 2018).

**7) Use and Adoption of Smart Services by Citizens (Success of Smart Services):**

A number of studies highlighted the importance of perceived security and privacy in smart cities services by citizens (Belanche-Gracia et al. 2015; Chatterjee et al. 2018; Cilliers and Flowerday 2014; Cilliers and Flowerday 2015; Van Heek et al. 2016; van Zoonen 2016). It was found that perceived security and privacy significantly affect the use and adoption of smart services by citizens. Studies differ on the extent of privacy concerns depending on the type of technologies, data usage and location. According to van Zoonen (2016) there are four areas of concern amongst people in smart cities that range from low levels (impersonal data, service purpose), to extremely high (personal data, surveillance purpose). The study explored how specific technologies (smart bin, smart parking), and data usage (predictive policing, social media monitoring) may produce various privacy concerns.