Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities

Chapter · April 2021

DOI: 10.1007/978-3-030-72139-8_2

6 authors, including:

Sabbir Ahmed
Jahangirnagar University
19 PUBLICATIONS **351** CITATIONS
SEE PROFILE

Md. Farhad Hossain
Jahangirnagar University
5 PUBLICATIONS **129** CITATIONS
SEE PROFILE

M. Shamim Kaiser
Jahangirnagar University
334 PUBLICATIONS **7,351** CITATIONS
SEE PROFILE

Manan Noor
Jahangirnagar University
8 PUBLICATIONS **538** CITATIONS
SEE PROFILE

Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities

Sabbir Ahmed, Md. Farhad Hossain, M. Shamim Kaiser, Manan Binth Taj Noor, Mufti Mahmud, and Chinmay Chakraborty

Abstract The smart city emerged as a model with the rapid growth of robust information and communication technology and the development of ubiquitous sensing technology. A smart city offers enhanced social facilities, transport and accessibility while promoting sustainability by using different sensors to gather data from the surroundings. The data collected can then be used to control urban infrastructure, such as traffic congestion, water supply, environmental monitoring, food services, and more. The smart city can track people's actions and deliver intelligent travel, intelligent healthcare, entertainment, and other services. Dynamic data change includes intelligent and systems solutions for the functioning of these networks to ensure confusion about events in smart cities. Recent advances in machine learning and artificial information allow intelligent cities to effectively deliver services through a reduction in resource consumption. Cloud-based machine learning models enable resource-restricted devices to interconnect and optimize efficiency. The emerging data collection and device designs are targeted at reducing energy savings rather than risks to privacy and security. Thus, the security and privacy concerns remain as intelligent city networks not only collect information from heterogeneous nodes which are the weakest link and susceptible to cyber-attack. In this chapter, we address security issues in smart city applications; and corresponding countermeasures using artificial intelligence and machine learning. Some attempts to address these protection and privacy problems are then presented for smart health, transport, and smart energy.

Keywords Artificial Intelligence · Machine learning · Security · Smart city

S. Ahmed · Md. F. Hossain · M. S. Kaiser (✉) · M. B. T. Noor
Institute of Information Technology, Jahangirnagar University, Savar, 1342 Dhaka, Bangladesh
e-mail: mskaiser@juniv.edu

M. Mahmud
Department of Computer Science, Nottingham Trent University, Clifton, Nottingham NG11 8NS, UK

C. Chakraborty
Department of Electronics and Communication Engineering, Birla Institute of Technology, Jharkhand, India

C. Chakraborty et al. (eds.), *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-72139-8_2

1 Introduction

The industrialization has made the city a central economic hub for any region. More rural people have migrated to urban areas for a better quality of life. As a result, both the population and the surface area of cities are rapidly expanding. This rapid growth requires structured management to deal with the problems created. The "Intelligent city" refers to an overall intelligent urban systematic structure. Smart cities are described by Harrison et al. as a group of natural environments, infrastructures, capital, facilities, social system layers [23]. It has been portrayed as an urban collaborative system that contributes to engineering, governance, maintenance, construction, services, and production of cities. Different smart city concept approaches have been divided into two paradigms, namely hard domains and soft domains. Hard domains are expressed as infrastructure, logistics, management of natural resources and mobility. Soft fields are expressed as culture, computing, schooling, politics, and government [29]. Smart city is conceived as a mixture of sensors and tags, embedded devices, interactive communication network and intelligent software. That is, smart cities are a broad framework for data generation from root level sensors, network integration, network collection, processing and compilation through intelligent computer software and information-based decision making to increase services and quality of life [5, 11].

The strict concept of a smart city was versatile and has also been used with various purposes and interpretations worldwide. The domains of intelligent cities are almost universal in various literature. These domains include economic and critical services, environmental services, education, governance, health etc. The areas covered above include traffic control, waste management, self-aware vehicles, weather protection, navigation, and natural disaster prevention. The expansive domains have rendered challenges such as data management and storage, communication, computing capacity, protection, and privacy. However, the key focus of intelligent cities has been the energy efficiency of sensors and mass usability. Rigorous and complex structures with adequate computing power are less common in these areas. In most systems, this creates a security weakness [18].

Smart cities rely on the Internet of Things (IoT) and user input as the data sources. IoT devices in smart cities are equipped with digital electronics, limited computation and internet communication capability. It also includes mobile phones, cameras, or devices that can record any surrounding data, Microcontroller, wireless technologies, RFID, and addressing are few critical components of IoT solutions [32]. Numerous devices interconnect to produce an expected result. Increasing the number of IoT functionalities and inhabitants generates enormous amount of data. An estimated 50 billion IoT devices are being added till this day [22]. However, server-based systems like e-commerce, online banking, and social media are also emerging as key components of smart cities apart from IoT technologies.

Traditional network infrastructure is inadequate for communication among devices, also for data collection. High bandwidth data communication, low power

consumption, and coverage area are the basic requirements for smart city connectivity. Various protocols such as MQTT, SMQTT, CoAP have been developed in past years for the demanding need. Recent communication technologies like Wi-Fi, Bluetooth WiMAX, and ZigBee are used to connect to the local routers. The 5G/6G connectivity is also developing to meet the ever-increasing demand for mobile devices. In this jargon of various types of connectivity, security invokes a significant challenge to maintain privacy [28].

Artificial intelligence (AI) plays a huge role in smart cities. Data from IoT sensors and inhabitants need to be processed before determining a verdict or prediction. Conventional rule-based algorithms are not sufficient for such an objective. Specifically, Machine learning (ML) has been applied ubiquitously in smart city applications [35, 37, 38].

ML is a data-driven approach that improves prediction spontaneously based on given data. Since services of most cities are planning; prediction-based ML has been used in computers and smart systems to learn from IoT or inhabitants generated information. Whereas network technologies and IoT are behind data collection, ML complies in automating to "smarten" certain services leveraging data. Biometric recognition and other security applications are mainly based on ML algorithms. ML classification and regression models are also employed in fraud detection, network security, encryption and encrypting, bot scalping prevention, malware detection, anomaly network packet, spam recognition, and many more. The average cost of a data breach is estimated as 3.86 million dollars [44]. Among these data breaches, malware attacks are increasing significantly. Figure 1 shows the percentage of the data breach by the malware attacks.

The major contributions of this chapter are as follows:

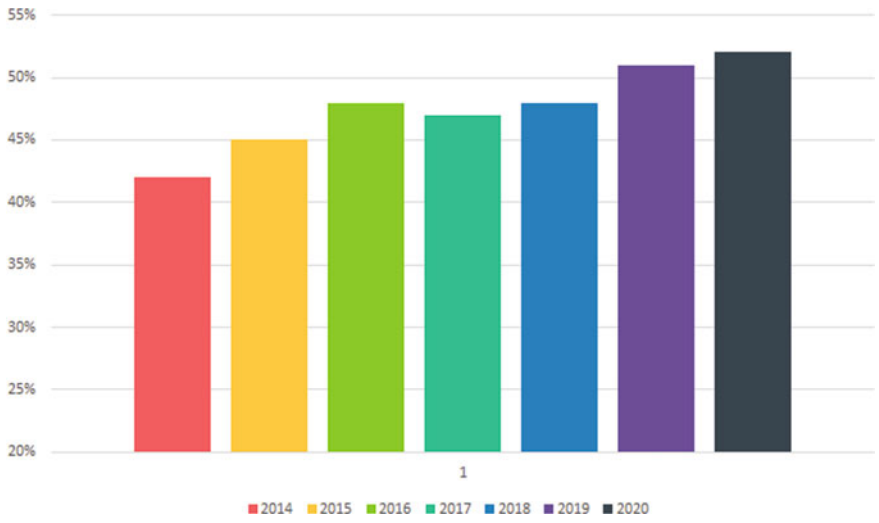

Fig. 1 Trend in data breaches caused by a malicious attack

– it identifies underlying technology for the smart city application,
– it addresses security issue in those technology,
– it reviews AI and ML based solution for security and privacy issue, and
– provides challenges and recommendations regarding ML and security based solutions.

The chapter is organised as smart city applications, smart city technologies, security loopholes in smart city, AI/ML based countermeasures open issues, challenges and recommendation and conclusion.

1.1 Smart City Applications

From remote controlling home appliances to detecting pre-earthquake, smart cities offer a broad range of applications. A smart city can be classified into few domains.

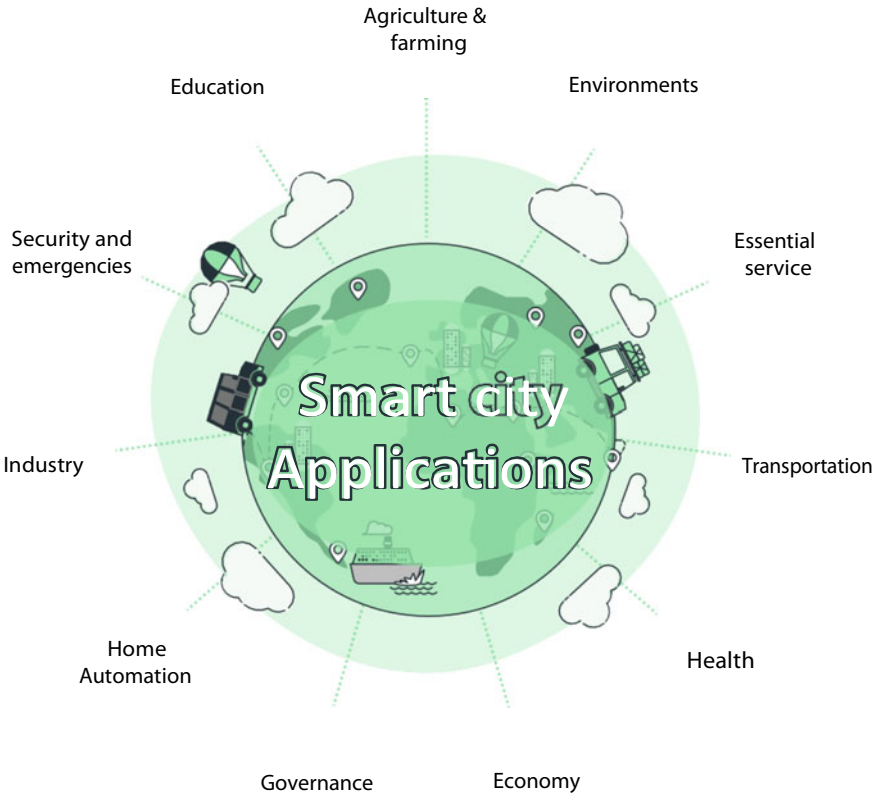

Fig. 2 Smart City Applications

Figure 2 represents different aspects of smart city applications. Detailed discussion about smart city applications is given below:

Agriculture and farming Smart agriculture and smart farming are the next big thing. Animal tracking is an essential aspect for controlling the quality and welfare management of a farm. For easy tracking, health monitoring, heat detection, eating habits monitoring and calving detection of the cattle; a proper tracking system is needed. Animal tracking solutions pave the way to greater production in farming by providing GPS, air tags and RFID based solutions. Monitoring the herd, finding the best time for insemination, separating sick cows, and admitting new calves to the system are taken care of with smart solutions. Farming systems are affected by global climate change and global warming. Production of plants can get decreased in the presence of hostile weather and different kinds of diseases. A smart greenhouse farming system can overcome this problem. In order to increase the production of crops, if a system can monitor the interior and exterior information of a greenhouse, it's called a smart greenhouse. If the season is dry, a smart greenhouse can provide enough shade and preserve the wetness to create a friendly environment. Controlling the catalysts needed for plant growth, preventing diseases, increasing the cultivating season, and maintaining a good quality of crops using necessary fertilizer ingredients are the key benefits of smart greenhouse. One of the significant developments in a smart city is golf courses. To create a good golf course, it is important to plant trees, track players, and have a good watering system. A sensor-based irrigation system can keep the grass green and well-drained in this context. In smart cities, the meteorological station network plays a vital role in ensuring weather forecasting in agriculture and farming fields. It can be used in different sectors as it provides air pressure, temperature, wind direction, rainfall and humidity. This information can be sent into the cloud for further processing. The location of the stations can change according to their objectives. Similarly, by increasing or decreasing the airflow and temperature, the smart compost system controls the handling of animal manure.

With adequate moisture and temperature control systems, the conditions of both green and dry weeds, left-overs from maize-stalks or other crops, hay, wood ash are taken care of. The system warns the user when it is appropriate to initiate the next move. The quality of wine is indeed the outcome of an extended collection of influences, including geological and soil conditions, environment and many other factors. The classification of grape quality and the amount of sugar in grapes play a critical role in improving wine quality. IoT solutions will define norm of cultivation and track soil humidity and other vital factors in vineyards [52].

Environment Environmental science and engineering can contribute to the study of the effects of climate change in urban areas by interpreting the connection between natural disasters and human-created pollution. The information acquired from social, economic, and technological stakeholders would help to establish an effective plan to defend against natural disasters. Further analysis of the data obtained can help define the bottlenecks in the current system. It will help to build intelligent approaches to plan for future real disasters and will assist people to respond accordingly. By incorporating AI networks in smart cities, researchers opt to develop and implement support structures in decision-making. After understanding and identifying the

problem statement, these systems typically acquire data from the respective fields and process the data to create interrelated information. Processed knowledge helps to make real options. And with a clear idea of the worst possible outcomes, the best candidate choices are implemented. It is prudent to detect fire through gas combustion, as forest fire emits gas but surveillance video data can also be used in this context by image processing. IoT sensors from designated forest regions may collect these data and intelligent communication links must ensure proper data flow. After processing the data according to an algorithm, the real-time transmission of information is accomplished with the assistance of wired networks or wireless sensor networks. When forest fire spread widely; rapid decision-making is required. To evacuate civilians, systemic fire safety, and information distribution among the actors who take emergency measures in handling wildfires, there must be a smart information sharing structure. Air pollution is man-made because air pollution is caused by fuel combustion, greenhouse gas emissions and contaminants used in fossil-fueled factories and power plants. By sensing hazardous gases, smart cities monitor air quality. Two types of sensors to monitor air quality are used. Two types of sensors are used to monitor air quality: mobile WSNs and stationary WSNs. By combining wireless sensors used in city buses and mobile sensor networks, real-time tracking is achieved. This system should be stable enough to function for a longer-term and deliver convenient outcomes with less upkeep. This system produces better result compared to other sensor-based detection systems [30]. The dense level monitoring consistency is achieved by monitoring snow dynamics and other complementary hydro-meteorological variables using the respective sensors. Authorities should take appropriate measures to avoid emergencies such as avalanches if the snow level and dynamic information expect anything terrible. So far, there are no systems to predict precisely when and where the next earthquake will hit. At the same time, the current system can trigger an alarm before the disaster. To safeguard the city, the system should be able to convey an indication of potential hazardous effects.

Essential services/utilities Water, gas, electricity, and connectivity are everyday human needs. Just 4% of the water can be used, which is why good management guarantees the best use of precious resources. There are also instances where water is wasted. For e.g., chemical exposure in water sources, improper public pool maintenance, leaking pipes, and flooding of rivers triggered by heavy rains or the rainy season. In tap and drinking water, biological and chemical pollutants trigger the development of infectious diseases. Hence, rapid and responsive identification techniques are essential for maintaining the availability of secure and clean water. The unhealthy water source impacts human health, causing diseases such as hepatitis, measles, SARS, gastric ulcers, pneumonia, and lung problems. There are many chemical pollutants in the water supply. Ammonia, chlorine, sodium, and sulfur are some of the instances. Such heavy metal dangerous compounds such as arsenic (As), cadmium (Cd), lead (Pb), mercury (Hg), and nickel (Ni) are also present in the supply of water. These non-biological contaminants are among the toxins that are widely found in metropolitan environments and represent a large spectrum of human behaviors. To detect biological contaminants, multiple tube fermentation (MTF) technique, membrane filtration (MF) procedure, DNA/RNA amplification,

fluorescence in situ hybridization (FISH) methods are implemented. Precipitation and coagulation, ion exchange, membrane filtration, bioremediation, heterogeneous photo-catalysts, and adsorption methods are used to combat chemical contaminants. In addition to water pollution problems, problems associated with salinity have been a concern since earlier civilizations, particularly in aquaculture. Instant salinity shifts have been explored among these issues. This is surely detrimental to marine creatures. A sensor tracks the water salinization of aquifers. The service enables us to figure out when and what makes fresh water to become saline water. The population of cities is rising every day and the waste is also growing. The increasing quantity of waste needs the collection and disposal of waste every day in certain central waste disposal areas. This can cause issues with traffic in busy cities. To mitigate these issues, sensor-based systems are used to avoid the waste from being collected on a day-to-day basis. Smart containers will contain sensors to measure the waste and send information to the central waste disposal administration. The administration would then decide whether or not measures are appropriate and take necessary steps. In other words, send waste collectors to collect waste or notify the authorities to repair containers. Smart containers can not only detect waste, but also can present it to people using IoT technology or a digital screen. This approach means that the system is more streamlined and requires less labor and complexity. However, the trash collector trucks can- not collect all garbage. There can be more considerable waste such as furniture and human-discarded household appliances. The environment protection will be guaranteed by a model to reduce the distance of waste from a disposal area, find an appropriate disposal route, and process the waste algorithmically using web-based and mobile communication. After the waste has been disposed of in some central waste area, significant attention must be paid to the waste processing and disposal according to the organized procedure for other environmental entities not to be harmed.

Security and emergencies The smart city ensures the safeguarding of possible risks for residents, organizations and other institutions. To protect city agencies and take responsible action in the event of emergencies, it needs to enforce protection measures. A zonal protection system is created by the intelligent way to address the safety measures of a city. This can be controlled through the access control perimeter. In a specific perimeter, all necessary safety measures details and possible threats will be visible. Authorities will be granted power over this region. The protection is strong enough to prevent unauthorized users from accessing the area. The detection of liquid presence is critical because sophisticated industries require water cooling systems. Also, data centers and systems that produce heat need a water cooling system. Thus, identifying the water/liquid presence is important so that all controls and devices are protected against possible destruction. If this can detect the amount of liquid, it will be adequate to hold different industries' mechanical systems, valuable domestic appliances, data centers from breakdown, and corrosion. Since humans are constantly exposed to environmental radiation, it is important to take into account a town's radiation level. And if there is more than the tolerable level of radiation, the citizen cannot tolerate the radiation. In addition, if any nuclear plant is located next to the city, security measures should be taken. A smart city should maintain distances

from the nuclear plants. There should be a well-structured system of emergency decisions. The radiation level monitoring systems would then analyze radiation data and help to determine where the leakage is to take protective steps. This system will not approve any future system that is a risk of radiation exposure to the city. In effect, the protection of people shall be assured by a smart radiation monitoring device [52].

Governance The smart city applications are classified into few domains. One of the domains is Government. This domain is also classified into more sub domains. They are city monitoring, e-government, emergency response, public service, transparent government and more. The local governments must monitor the government provided services to ensure the proper execution of the city services. To improve citizens' quality of life, water system management and electric grid monitoring can be done in real time. Heterogeneous sensors can be utilized to monitor public places. The government's use of ICT is called e-government in the correspondence and provision of public services. Risks are defined as effective government policies, and awareness of the art of management. The success factor is studied using multiple forms of campaigns. Better transparency and judgment with continuing coordination are important factors for governance. To face this challenge, an open and anti-corruption tool is provided as a transparent government [8].

Economy Sustainable and stable economic development can be accomplished in a smart city. It provides numerous economic benefits to its residents. The citizens of smart cities aim for the efficient use of natural resources and acknowledge that their economy will not succeed indefinitely. "Sharing economics" has arisen as a modern economic or business paradigm within today's digital culture. As a service, people and organizations use under-utilized resources and make revenue by "sharing economics" [50]. The efficient utilization of ICT across all the city's economic activities makes the economy "smart". The combination of smart city and smart economy is visionary. The universal use of high-speed internet is the prerequisite of smart economy in smart cities. For all aspects of their lives, the psychology of people accessing the internet produces possibilities in e-commerce. The integration of smart energy grids and smart metering with sensors and other instruments ensures proper delivery and reliability of the network. The smart economy of energy guarantees effective monitoring of power and energy quality. AI-based e-commerce applications ensure automation in this field. ML is now allowing e-commerce-based businesses to process consumer data, promote the most relevant products, and simplify customer service through chatbots.

Education The advancement of emerging technologies enables smart cities students to interconnect with cloud resources efficiently. Smart city functionality depends on user capabilities to engage in tech-driven environments. Smart education is the prerequisite for smart citizens. Recently global pandemic has shifted class and study material to online. Educational applications in smart cities include smart learning, distance learning, smart pedagogy, e-learning, etc. Smart pedagogy is multi-tier and includes a framework for class-based, group-based, individual-based and mass-based learning strategies. In order to create interest and intuitive perspective amid learners, games like Urban data game can be utilized. Educational services

should be a knowledge collaborative approach instead of a business focused institute, which will provide smart cities with intelligent citizens.

Home Automation Smart home refers to wireless or automatic control of appliances and attributes like heating system, water management, light, energy, alarm, speaker, surveillance and so on. Sensors are placed in the home appliances for collecting related data. This data is preprocessed with a microcontroller to produce measurable value in known unit value and send to a central hub. Automated decisions are made in the microcontroller or central part of the system to efficiently and effectively run those appliances. Information also uploaded to cloud for users being able to do changes if needed. Sensor data also help to keep track of any incident like leakage or fault in each individual system. User interface also provided for smooth interaction with users. Light, air conditioning, water pump, garage door, refrigerator, home router, speaker, toaster are some devices that are controlled in such a way. For device to hub connectivity, low power methods like Bluetooth and ZigBee reduce power consumption of sensor devices. In case of home network outage, home security devices like smart door lock, intrusion, surveillance camera tends to use cellular connection like 4G/5G.

Transportation A fully autonomous vehicle is thought to be one of the key features in smart cities. In recent years smart city inhabitants grew large in number which in turn created traffic problems like congestion, speeding, accidents and thus services like navigation became necessary [7, 9]. Human or driving error is the main culprit behind most of the accidents and congestion. Total number of vehicle crashes in the United States of America is estimated at 55 million with 277 billion dollars of economic cost; whereas for 93% of the accidents human error turned out to be the primary reason. Again, bad driving skills are the main reason behind inefficient parking and traffic congestion. Hence, full autonomous vehicles with satisfactory levels of accuracy are required in smart cities. Since full autonomy is currently not fully developed and human interaction can be obligatory in some situations, semi-autonomous solutions like driving assistant systems are work in progress even though they have been implemented in some vehicles [54]. Total traffic management systems in smart cities include adaptive traffic light, vehicle to vehicle communication, advance breaking, path planning and navigation. On-board and roadside sensors like LIDER, ultrasonic, infrared and video feed are common for these scenarios.

Other fields of application include health services [13, 19], industry, retail and other facilities. Smart health utilizes IoT, wearable and monitoring technologies to keep track of individuals. Mobile health which is a part of smart health collects information from mobile devices mostly smartphones, enabling health emergency tracking. Patients can be treated from another part of the world using low latency real time data transfer [27, 36]. Smart city industries are built on the basis of low carbon and waste emission. Reusable energy and resources are the main concept for the smart city industry. Smart city technologies are on the rise, new areas are introduced daily. Thus, a thorough explanation of each program is beyond the reach of this chapter of the book.

1.2 *Technologies Used in Smart Cities and Integrated Technology in the Smart City-Edge/Cloud*

A broad number of interconnected and constant evolving technologies enables smart city application to be feasible. Textual and practical invention has been occurring for the past few decades in the field of smart cities. Enormous smart city applications perspective has been a major force that incites researchers to exploit new innovative solutions. Figure 3 represents an abstract view of smart city technologies. Key technologies behind smart city application are highlighted in the following sections.

Data Acquisition Data acquisition in smart cities primarily depends on IoT sensors, user input, and historical data. Data acquisition is the method of acquiring and gathering data from different entities. These entities consist of end users of services provided by the smart cities and sensing devices.

Fig. 3 Technologies used in smart cities

Inhabitant Engagement: Inhabitants engagement in response and feedback services of smart cities represent user experience with the services and how to improve those services. These user reviews reduce testing costs and amplify the quality of services significantly. More extensive sustainable development strategies need to be developed that promote people and consumer participation to leverage the co-creation of expertise, cooperation, and empowerment.

Fields like waste and utilities management services need smart citizens since they can be seen as utilities rather than problems to be solved. Citizen participation provides important insight about future scalabilities, such as the damp housing problem. Data acquisition from citizens removes expensive sensor-based data retrieval and provides a more intuitive perspective on challenges and their solutions. Mobile applications like google pigeon use crowd sourced instantaneous data to notify users about the current traffic condition of mass transit in cities. In this era of virtualization, user -posted information in social media serves as a great source of information and latest news media of the twenty-first century. Such mobile crowdsourcing methods can be developed for function ratification and user engagement. User sociality, the distance among users and activities and fog computing-based user engagement improves functionality of smart city. A TOP-SIS (Technique for Order of Preference by Similarity to Ideal Solution), Entropy, and AHP (Analytic Hierarchy Process) dependent framework have been developed by Ahuja et al [2] for smart city data acquisition.

Sensor and IoT: From large viewpoints, sensors are entities that record events of surrounding environments. Sensors used to be heterogeneous in nature, the architecture and the results varied in large ranges due to specific application domains. In smart cities sensor data with different fields used in a homogenous nature to determine homogeneous solution. Sensing technology is a vast field of material science. The common features among these technologies have been electrical output which is generated in direct correlation of the events or circumstances. Dissimilar metal with higher thermal conduction and electrical conduction can be used as a temperature measuring system. Temperature sensors also can be built on semiconductor, thermocouple, thermistor, resistor or infrared basis. Photoelectricity, Induction, and capacitors are utilized in proximity sensors to detect motion. Elemental characteristics of materials are applied in infrared, ultrasound, humidity, accelerometer, gyro meter and optical sensors. Chemical characteristics-based sensors are utilized for measuring certain behavior of soil, gas or water. Imaging techniques also used for video/depth data. Electromagnetic wave-based RFID, NFC sensors are used for identification tasks. Sensors are everywhere; from sound-vibration to fluid, flow, radiation, navigation, force. Every measurement available to human kind is automated with sensors. The methodology of sensing technique is vast and behind the scope of this textual analysis. Estimated 8,583,503,168 bytes of data can be acquired from small sensors without regarding audio or video feed in a smart city [47].

IoT is the integration and interaction of entities on a global basis. Though each entity's sensing data may be insignificant, the collaborative approach can lead to good and cost-efficient optimization of smart cities' services. A huge investment of resources has been made for IoT infrastructure in smart cities since it is thought to be

the next big revolution from a technical perspective. These entities include devices, sensors, embedded systems, computational machines and so on. IoT consists of three-element; hardware: assembled with sensor, device; middleware: made with storage technology and network; presentation: consists of processing technology and visualization. Because of the interdisciplinary characteristics of IoT, various aspects of its ideology is depicted by different authors. IoT can be also described as a combination of wireless sensor networks, middleware and network, cloud computing and application software. From the smart city perspective, IoT is integration and infrastructure with many research topics that enable the application to be made upon input variables. For instance automated surveillance, audio watermarking schemes, stenography protocols, harmony search algorithms for medical perspective, grey relational analysis for forecast, thermal rating of network transmission etc. can be deployed in smart cities. From the provided services viewpoint, IoT infrastructure can further be divided into service back-end infrastructure, machine to machine connectivity, hardware-specific software platform and software extensions. Technologies like RFID, NFC for user authentication, smart vending machine, tracking and monitoring system, smart object semantic system, service composition, augmented reality, smart scheduling, access control, event processing, intersection control, mobile sink, proxy cache and virtual machine using IoT can also be utilized in smart cities.

Network and Communication Technology Data needs to be sent to a central platform to be processed. Sensing and collecting devices are low power consuming and less computationally expensive. These devices are built for vast deployment strategies, not for in device processing. Though devices can provide data points at a higher rate, and the receiving end also has a higher acceptance rate, the communication medium works as the bottleneck for the whole system. Traditional communication medium limits data rate and hinders the continuation of the process. Packet loss, high latency are the main obstacles for communication systems in smart cities. Thus, communication technologies play a huge role in connecting devices as higher data rates and range enables new technologies to emerge. Streaming services are a perfect example of sharing high-quality real-time video feeds. The communication technologies are also needed to be compatible with various sensor devices. Though most of the components rely on wireless technologies, wired communication is also used in place of network-intensive signal processing. Wired transmission medium includes Ethernet, optical fiber, coaxial cable. Optical fiber is the most improved wired technology for long-distance, high bandwidth transmission and currently serves as the backbone of modern internet infrastructure. The robustness and scalability of adding new devices to the network have made wireless technology the standard of smart city communication. Wireless technologies can further be divided on transmission range. For a short-range machine to machine (M2M) communication Bluetooth, Zigbee, Z-Wave are quite common in small network sensors connected to a local device. These technologies range from 0 to100 meter. Recently developed LoRa, Sigfox, NB-IoT, Weightless has shown promising results for communication up to several kilometers. LoRa offers a combination of longer distance, power efficient and safe data transfer. The Sigfox uses power while transmitting data and covers long distance (up to 20 km) for IoT devices. Despite of the advantage of these technologies Wi-Fi remains the

holy-grail for wireless communication. Smart devices like home appliances, smartphones, automation systems, TV etc. are connected to local routing points leveraging Wi-Fi technology. Wi-Fi offers multiple frequencies with good transmission range, high bandwidth and availability in most of the devices made it one of the most prominent transmission technologies in smart cities. Even most of the services in smart cities offer free Wi-Fi in order to connect users to the internet. WiMAX technology is for long rang and works as a backup for wired communication.

Cellular communication is also common in smart cities, since it has better mobility. Cellular communication is mostly provided by private companies and mostly available throughout the globe. Previously discussed technologies use a central access point for communication and these technologies are not built with the mindset of a network of access points. As a result, device with mobility suffer inefficiency moving away from the access point since the signal deteriorates relatively to distance. Hence cellular networks provide ceaseless transmission to mobile devices. While 5G connectivity is built upon most of the cities, a fully functional version of 5G is yet to come. 3G and 4G evolution familiarize the concept of IoT and smart cities to citizens. Long Term Evolution (LTE) 4G network technologies are still in operation for most of the smart cities due to its high reliability, low cost and geographic availability. 4G support speeds up to 14 Mbps that is sufficient for most of the IoT sensor devices that communicate with text data. Though 4G has drawbacks that are not acceptable in smart city concept. Several systems have strict latency limitations which LTE does not easily meet.

5G on the other hand uses millimeter waves for high energy and data transmission. 5G is thought to be the next generation network transmission technology. Large corporations and cities have taken initiatives in order to implement 5G. Real time data transmission with higher bandwidth, efficiency and security over 4G are the key characteristics of 5G. Real time IoT, Internet of smart vehicles, intelligent transportation system, personal home assistant, augmented and virtual reality are some of the features of smart cities which will be enabled by 5G. Though these services are more likely to be implemented with 5G; new innovative services and products will appear if the date rate, latency, number of connected devices improves significantly with 5G. 5G technologies also thrived on developing sub domains like enormous multiple input, multiple output, device to device communication and small cell networks.

6G is a conceptual network technology, though ample initiative has taken this scope, exact architecture, infrastructure yet to be known. 6G is thought to be not only high frequency high speed connectivity but also intelligent network leveraging ML and algorithms. Speed is projected as several Gbps and latency as low as microseconds. Multisensory XR application, intelligent robots and autonomous systems, brain computer interaction, self-sustainable network, smart surface and environments are some of the applications envisioned as 6G services [1, 28]. Real time online medical services and internet of healthcare things (IoHT) are expected to enable e-health services to its full form [5, 10, 14].

Cloud Computing Cloud computing refers to data storage as well as processing, running applications on stored data to obtain a certain output. Cloud computing has been a principle technology to provide users with high-level applications in small,

power-consuming and less computational expensive devices. Again, large files have been accessible through cloud services, lessening the burden of placing large chunks of memory in mobile devices. Another factor of adopting cloud technologies in smart cities is the sheer amount of data generated, collected, and analyzed by leveraging IoT technologies. A computationally costly security program can run easily in a cloud server and also ensures user privacy and security without having trouble managing these applications on the device. Large data centers also provide new media for content consumption and sharing for smart citizens. Contextual data of smart city inhabitants can be stored, processed, and visualized in cloud servers. Contextual data management has been a huge issue since user profiling and exclusion is difficult in certain perspectives. To solve this problem, a layered cloud architecture for context aware citizen services has been proposed [31]. Again, cloud services gather and store different types of data from various sensors, actuators, and devices. This heterogeneity leads to difficulty in receiving, organizing data for any potential use cases. Management, control and automated analysis of data is required for distributed cloud services. Cloud combination, network management, sensor IP network and sensor control are needed for such technology. Through cloud portal and taking feed, city governance management creates new possibilities for Government cloud (G-cloud) services [11, 26].

Edge Computing IoT devices simultaneously generate data in smart cities and send them to cloud services utilizing communication and network technologies. Extensive data collection and processing in cloud services require costly data centers and infrastructure. An obvious solution to this problem is to process data at the device end. Edge computing refers to such computing systems that occur on the edge of a network. Edge computing sometimes collides with fog computing terminology, whereas edge computing mostly focuses on the device side and fog computing on the intermediate infrastructure side. Energy management and scheduling for IoT smart grid technology with edge computing reduces network usage and processing time. Smart citizens use smartphones to be connected with cloud services. Mobile edge computing schemes can achieve continuous latency-free services without location consideration, because data size reduces due to preprocessing. This preprocessing deduct unnecessary data, and only relevant data is transmitted. Hou et al. utilized a wireless mesh network for collaborative edge computing and proposed the green survivable virtual network embedding [25]. Besides pre-processing device data in the sensor network, devices can dedicate their idle time for whole network processing.

Software Defined Network Smart cities generate intensive data that needs to be passed through communication networks. Perpetual accessibility through communication network requires to maintain the traffic. Due to any emergency, network overload becomes critical to services. Software-defined networks (SDN) use priority-based algorithms to cope with routing issues in smart cities. Again in natural disaster events, lives depend on capabilities of network to convey victims' messages to the emergency responders. Customizable demand, functional virtualization for data and intelligent mechanisms for controlling the infrastructure using software stack can be used to construct such SDN ecosystems. Again by controlling processing delay of network components using an intelligent engine, virtual mesh topology and fog

unit; much reliable communication can be possible in emergencies. Traffic management; another key aspect of smart cities consists of traffic lights, signals and cameras where network overload and delay can create massive traffic congestion. Multiple SDN-based smart power grid control has been reviewed by Rehmani et al. [42] on the scope of privacy and security. Since SDN operates network reliably and securely, utility services like smart city power management have been dependent on SDN to function correctly [4, 18].

Block Chain Blockchain is a data storage mechanism that records and distributes data throughout the network, which makes it almost impossible to unauthorized manipulation. In distributor server networks called microservers, the block chain stores data with exact hash value and retains authentication between the main transaction server and microservers. IoT sensor transmission in networks often contains private and sensitive information about the important city services. Any temperament of data disrupts the flow and control of services that citizens directly depend on. In this regard, smart cities require effective sustainable solutions to ensure security for device communication. Key characteristics of blockchain technologies are decentralization, persistence, auditability and anonymity. Ever increasing security threat has been a key factor for utilizing blockchain in smart cities. Though a number of recent cyber-attacks have cost millions of dollars [40]. A number of cyber-attack case study and prevention methods has been reviewed by Li et al. [34]. Security framework can be developed using blockchain technologies in physical, communication, database and interface layer to secure specific layer attack. In a smart city context blockchain can be utilized in smart healthcare, smart transportation and traffic, smart grid, personal data exchange, supply chain management and other essential services. Sharing economic resources among smart city inhabitants provides social stability. Technologies like online banking and mobile banking have been the most relevant method for transactions in smart cities. Such blockchain-based secured sharing economic framework is required to ensure safety and privacy of smart and mobile banking users. By exploiting the power of new software-oriented networking and blockchain technology, a hybrid network model for the smart city can enhance security and privacy systems.

Big Data Smart cities produce large volumes of data in their everyday activities. Advancement of IoT, sensors, mobile devices and network technologies crowded the servers with data from both users and mechanisms. These avalanche of different sorts of data need to be managed and analyzed in mostly real time. All of the mentioned characteristics of smart city data matches the perspective of big data technology. Hence precise analysis and systematic processing of heterogeneous and complex data in smart cities positioned itself in big data technologies. Well thought out processing mechanisms give interesting insights and patterns of a smart city. Big data and computational resources will also be leveraged by cities to increase the quality of municipal processes and utilities. Big data expansion moves the focus from extended planning process to brief analysis on how cities operate and can also be managed. Volume, velocity, variability, variety and value has been referred to as the key points of big data in smart cities. Big data modeling and research focused from a theoretical point of view on smart cities by introducing a Cloud-based analysis service which can be

further built to produce intelligence information and facilitate verdict throughout the context of smart urban spaces. The big data architecture can be divided into data acquisition layer, data mapping layer and interactive application layer. Hashem et al. expressed big data technologies as business analysis tools from smart city data and analyzed its effect on the city of Copenhagen, Helsinki and Stockholm [24].

Artificial Intelligence and Machine Learning The phrase "AI" was first used by computer scientist John McCarthy as "the science and engineering of making intelligent machines" [48]. AI is the computer science branch where the main focus is making machines conform like people, primarily improvising machinery's intellectual skills and designing smart devices. Intelligent methods for optimizing output parameters are meant by ML using datasets or previous learning experience. In particular, ML algorithms construct behavior modeling on broad data sets with mathematical models. ML also helps to learn without explicit programming. These models are used to generate future projections based on new data. ML is collaborative and has origins in many fields, including AI, optimization theory, information theory, and cognitive science.

ML is a subset of AI that focuses more on learning patterns in the given data. AI is used to enhance security mechanisms in existing structures by frequent use of the IoT. With AI integration, the current systems are now more powerful and smart. For video monitoring and analysis, Unmanned Aerial Vehicles (UAVs) is crucial in smart cities' security initiatives. AI is also used for gunshots detection. In intelligent cities, UAV must be the most innovative initiative, considering a wide range of areas integrating AI applications. It can be used in smart cities to monitor traffic, to manage crowds, fire control, civil monitoring, and border defense [3, 48, 49].

1.3 Security Loophole in Smart Cities

Since smart city has a network architecture which is vast in nature, cyber-attack can be devastating by ceasing the essential services. A huge stream of continuous data made it even harder to maintain privacy and security. Most services in smart cities are shared among citizens. Privacy conserving and trustworthy mechanisms needed to survive potential attacks leveraging shared data. Data acquisition occurs in the sensing layer from sensors, accumulators, devices, and citizens. The access layer is the communication technology related to the transmission of data. Cloud and big data technologies mostly fall in the domains of the processing layer. Some of the previously mentioned technologies like blockchain, SDN, network function virtualization, IoT, AI, and ML provide and resolve security issues throughout the smart city infrastructure. Hence a layered analysis on security and privacy issues regarding these technologies has been provided for better understanding. Figure 4 depicts this layered analysis as well as the related technologies.

Perception layer Smart cities collect data from physical objects and events. Perception layer in smart cities consists of physical nodes and machine to machine networks. Tempering these physical objects results in security concerns. Sensing

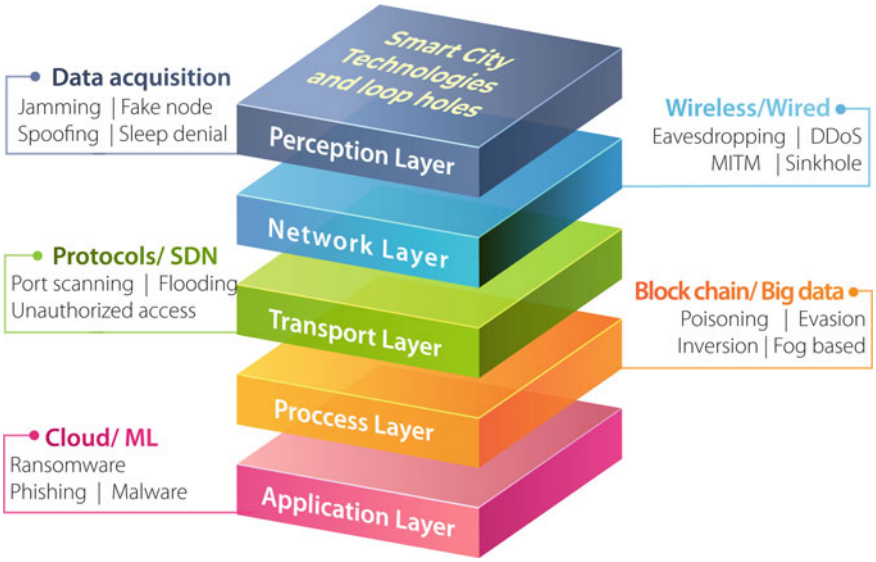

Fig. 4 Smart City Technologies and loopholes

layers also deliver heterogeneous data; finding anomalies in this vast range of data types are quite hard to consider. Lack of common standard for M2M communication endangered the system mostly. Wireless sensor network communication can be hindered with unwanted signals or jamming in which WSN devices can not differentiate necessary signals. RFID, Zigbee or Bluetooth M2M communication are most vulnerable to this type of jamming. Jamming can further be divided into constant, random, deceptive, reactive, shot noise-based jammer and almost all of these types of jammer contain a noise signal ratio similar to target network traffic. Attackers can also replace sensors with malicious devices which send similar but harmful data streams to layers upward resulting in total network failure. This type of fake node also can be created by interrupting and modifying sensor output. Garbage control signals are sent into sensors so that these sensors cannot go to the sleep stage, consume power simultaneously and result in power shortage. Sensors are made to be awake for an extended period of time thus this type of attack is called sleep deprivation attack.

Network layer In network layer, attacks are projected to redirect into wrong routing ways, network traffic congestion. Denial of services (DoS) and Distributed denial of services (DDoS) is a shortage of network computing equipment and capabilities. In the network layer, the transmission medium is flooded with signals from the attacker thus stopping essential signals to pass [33]. Botnet is created by affecting real users and uses their credentials to congest the system. On the contrary, eavesdroppers record signals in networks and utilizes this information without consent of the source. Multiple such eavesdropper's collaborative approaches can result in privacy issues for users since they might be able to decode the complete message.

Attackers can make a routing node more attractive and list shortage path possible for every routing enquiry. Thus, it receives all the routing requests from surrounding nodes and incoming packages, thus packet loss happens indefinitely which is also called sinkhole/wormhole. Intermediate messages can be interrupted and rearranged to create delay and congestion in the network. This interruption between two nodes enables ejecting malicious code into a network which is also known as man in the middle (MITM) attack.

Transport layer Transport layer contains the protocol for communication (UDP, TCP) for smart city networks. The method to determine the target program's communication ports is port scanning. It allows attackers to list down the clients who are connected to a specific service through a specific port. Data flooding is a method that overwhelms the protocol with data which in turns overflow the system also used to attack in the transport layer. Data is sent until the data protocol is exhausted and stops working. Unauthorized access to the network can inject malicious programs to the system.

Processing Layer Processing layer enables computing algorithms to process data into information. In the processing layer ML based methodology is deployed to clean data or learn from it. By changing test and training data of ML models, the model eventually learns ambiguous patterns. This type of data tampering is also known as poisoning. As the software industry improves, so does the malware. Recent malware attacks cost millions of dollar for smart cities and malware evasion which is hidden executable file throughout the network, becomes more prominent to occur.

Application Layer Application layer of smart cities is the most vulnerable in a sense that it interacts directly with the user and is easy to access. Application layer attacks include phishing, Virus, Worms, Trojan Horse, Spyware, Denial of Service (DoS), Software Vulnerabilities, malicious script. Phishing refers to data theft by exploiting user stupidity. A link similar to user services is created and sent to the user to fill it up; tending the user to give up valuable personal information. Software and web application vulnerabilities are easy to be found out by the attackers as they can test the systems. SQL injection based cyber-attacks are also common in this regard. Many smart cities use out of the date security software and encryption methods that are too easy to be exploited. Even more secure methods like block chain [34] have been also prone to cyber-attacks. Many bitcoin-based services faced the same problem and millions of dollars have been stolen. Moreover, vulnerabilities in SDNs permit attackers to hide their identity in the system and observe the behavior of the system using the backdoor of SDN. Not all of the smart city systems use the above-mentioned layered approach. Edge-cloud-fog based IoT systems are also quite common. The vast scale of crowd architecture and big data itself creates security and privacy concerns which are yet to be seen in smart cities.

1.4 AI/ML Based Counter Measures

AI-based algorithms, specifically ML, have shown great success in detection, recognition and regression-based tasks. Most of the application of AI/ML in smart cities gleaned on various attack detection and prevention tasks. So, it is safe to say that AI/ML based counter measures are applicable in the scope of security in smart cities. Some of the countermeasures for previous section's security loopholes are following:

Perception layer Attack in the perception layer focused changes in physical devices and entities. Physical device authentication to the network provides information about such anomalies and prevents unauthorized users. Such IoT device authentication framework has been proposed by Das et al. [16] leveraging Long Short-term memory. Long short-term memory works on time sequence data and finds out the imperfection in the output signal of IoT devices to deter- mine authentication error. Feature extraction can also be possible from channel information in Wi-Fi signals using deep learning algorithms. Human action uniquely miss-matched with one another; leveraging this fact authentication has been done. Physically unclonable function has been suggested for authenticating transmitter and receiver radio frequency in wireless nodes using in-situ ML algorithm [15]. 99.9% accuracy was obtained by authenticating 4800 devices amid changing network circumstances. Recurrent Neural Network (RNN) and Long Short Time Memory (LSTM) have shown sufficient improvement in solving Natural Language processing and audio-based problems. IoT device based human authentication from breathing sound might be probable as well using recurrent neural networks.

Network layer A DDoS attack method based on a support vector machine (SVM) classifier is built in the SDN. The DDoS attack method is prepared with a combination of SVM classification algorithms and extraction of 6-tuple characteristic values of the switch flow table [55]. For business networks, a combination of host and network intrusion detection systems can be combined as a SDN-built hybrid safety platform. A hybrid IoT model is presented by incorporating the advantages of SDN and Fog computing. This model supports applications which require extremely low and predictable latency by analysing and assessing data at the edge of the network, which also improves network scalability and performance [51]. For wireless network sensor network (WSN)'s security against DoS attacks, a multilayer perceptron based media access control (MAC) protocol can be utilized to detect real time attack. DDoS attacks in the SDN-based environment can also be addressed using the SVM classifiers. In order to detect DDoS attacks, traffic information should be sent to the intrusion detection system. A hybrid ML algorithm based on bijective soft set approach, with combination of a proposed model results in detecting malicious and anomaly traffics [45].

Transport Layer In a smart city environment, data is stored on a cloud based distributed system. Single server system failure can cause service outage throughout the city. Data distribution is a key point in the transmission layer. Due to the abundance of labeled training data attack detection in supervised fashion often results in ambiguity. To solve the issue Rathore et al. proposed an ELM-based semi-supervised

Fuzzy C-Means (ESFCM) classifier [41]. Implemented on fog server, the proposed classifier can provide security and detection in case of distributed attack. Edge network shifted workload to the device end for faster communication and pre-processing. To ensure security issues on edge server device activity detection has been developed with Fuzzy C-mean classifier [21]. To achieve clusters that distinguish benign traffic from harmful traffic, Classifier has been deployed. Supervised learning methods such as statistical learning, SVM, sparse logistic regression, semi-supervised learning, decision and feature level fusion and online learning method has been deployed in the domain of smart grid attack detection by Ozay et al. [39]. They concluded that despite having less complexity than batch algorithms, online algorithms for real time detection work well. Distributed attack detection using deep learning and custom fog-to-things based algorithms are also deployed in smart city architecture.

Processing layer Intrusion in processing of data is a major threat to smart cities. A network Intrusion detection using anomaly and ML framework has been developed by Viegas et al. [53]. Which only used 46% energy compared to existing software solutions. Intrusion is mostly detected by using structured data related to the subject program, or a chunk of that program. Since this data varies with time, LSTM-RNN classifiers are best fitted. Similar Random neural network-based architectures have been developed for anomaly detection [43]. Neural network models like random forest, SVM can also be utilized in modern attack features learning. These algorithms work in the cloud services to detect abnormality on the network traffic in order to classify any anomaly or intrusion.

Application layer As previously mentioned, application layered-based attacks are most common, and ample research is done in ML to resolve security issues. Multidimensional Naive Bayes and SVM based classifiers have been developed to secure citizens from news media sources. Smartphone technologies enable smart city inhabitants to access information easily. To secure city services from malware stored in the user side, detection algorithms are being developed. Random forest classifiers, linear SVM and deep learning algorithms are exploited for these tasks to detect malware in wireless multimedia system SVM based detection and suppression model has been developed by Zhou et al. [56]. They compared the model with infected nodes using dynamic differential games. Distributed SVM and deviation in measurement has been applied for faulty data injection attack in smart grid [17]. For processing in contrast to x86, ARM architectures provide efficiency in IoT for its big-little design and energy efficiency. Deep RNN with LSTM has been useful to analyze execution code of ARM IoT device for malware [20]. Deep eigenspace learning has also been proposed for malware and application classification [6] by Azmodeeh et al. This architecture also provided security against junk code insertion. Learning-based deep-Q network for health- care security and privacy has been discussed by Shakeel et al. [46]. Generative Adversarial Network is gaining attention due its robust nature. Recent uses of GAN in anomaly and intrusion detection have shown great results. Combined frameworks like blockchain and ML provided overall security to the whole smart city cyber-physical system.

1.5 Open Issues, Challenges and Recommendation

In this era of information technologies, every information has been shifted towards cloud-based architecture. Smart city concept is to collect and manage information that is crucial to human life. This digitalization also creates virtual vulnerabilities like different kinds of cyber attack and data breaches. According to IBM [44] primary targets of the data breaches are personally identifiable information, intellectual property and corporate data; on average, 280 days are needed to identify and contain data breaches. Personal information such as email, phone number and passwords are shared or sold on the web by hackers. Big corporations like Google, Facebook and Twitter also faced data breaches. The recent data breach has leaked roughly 50 million Facebook profile data [12]. In contrast to this, smart city data are more sensitive since human life is directly dependent on smart city applications. As examples, data abnormalities in transportation systems may cause unnecessary traffic congestion and even accidents. Data breaches in power stations can cause a power outage that directly create complications in essential services like medical and emergency. Even most of the cyber attack's damage done by cyber-attacks are in the health care sectors [44]. Incorporating blockchain technologies with network architectures has shown promising results as prevention mechanisms in applications like health care and power sectors [34].

On the other hand, the burst of IoT technologies in smart cities also invokes securities issues like sending false data and physically damaged sensors. The large scale and heterogeneity of the sensors cause problems for universal security solutions. Moreover, most of the cloud infrastructure used in smart cities are provided by third party companies. These cloud servers are located worldwide, and little changes can be made only if permitted by local law. The regulation also needed for smart city mobile, web and computer applications, where potentially insecure applications can be filtered out. Intelligent, secure mobile devices and dynamic networks need to be deployed to ensure citizen data security.

Heterogeneity in network architectures is also an obstacle for smart city securities. Connectivity has been built around existing technologies with upcoming ones. Integration into the 5G network from 4G is still a significant challenge for smart cities since most of the devices are 4G capable. Different protocols in different connectivity layers also caused security analytics problems to figure out the optimum solutions. Again network infrastructure in each layer is provided by various companies, which prevents developing a unified and secure networks frame-work. Information received from the previous layer is thought to be authentic by each of the layers. Most of the mechanism exists focused on layer anomalies. Thus inter layer anomalies detection challenges also exist. Security vulnerabilities in new technologies need to be found out by the researchers before these have been used as a method for data breaches and cyber-attacks.

The tremendous amount of generated sensor and user data has also been a key challenge. Malicious data can be mixed up with the user-generated data. Behavioural and moral issues of the smart city inhabitants also raise security threats. Thus the

classification of data is needed, based on necessity in the smart city ecosystem. Again technologies like big data and ML must be integrated with security systems to manage the exponential increment of user data.

Most of the articles mentioned in the previous section are based on detection based countermeasures. Detection reduces the overall damages, but prevention is needed more to annihilate security threats. Very few works have been done so far for attack prevention. Preventing cyber-attacks may be deployed as a prediction algorithm that may classify incoming user data as malicious or benign. Context-aware ML models are needed to develop for real-time attack detection and prevention. Attention mechanism has provided amazing results for natural language processing which can further be used to generate sequence to sequence programs to tackle detected malware. Most algorithms detect behavioural anomaly in system components. Thus faulty systems can be classified as malicious. ML models should be capable of distinguishing between faulty systems and malicious systems. The M2M communication technologies should further be extended, so redundant devices can take the workload of infected or attacked devices. Fail proofing of essential services in cases of any types of attacks also an exciting field that needed to be exploited.

1.6 Conclusion and Future Scope

Security and privacy are a concern for smart city applications. The services offered by smart cities can directly relate to the lifestyle of their people. Any kind of disturbance due to security issues may be fatal. Traditional security management strategies are inadequate due to the immense amount of heterogeneous data and thus service management is a monumental task. Security countermeasures based on AI and ML can be used in smart city services due to the availability of vast volumes of sensor data. This chapter discussed the concept of smart city and its services, technologies used, security threats and AI/ML-based counter- measures with some recommendations for future perspectives. ML is a critical component to solving unforeseen complications in order to sustain a stable smart city. Still some of the challenges and issues in this context constitute attack prevention, real time detection and integration of ML with network and cloud based technologies etc. The pursuit of developing ML technologies to conquer the challenges will integrate different aspects of smart city as an overall system.

References

1. Afsana F, Mamun SA, Kaiser MS, Ahmed MR (2015) Outage capacity analysis of cluster-based forwarding scheme for body area network using nano electromagnetic communication. In: 2015 2nd international conference on electrical information and communication technologies (EICT). pp 383–388. https://doi.org/10.1109/EICT.2015.7391981

2. Ahuja K, Khosla A (2019) A novel framework for data acquisition and ubiquitous communication provisioning in smart cities. Future Gener Comput Syst 101:785–803
3. Akhund TMNU et al. (2018) Adeptness: Alzheimer's disease patient management system using pervasive sensors-early prototype and preliminary results. In: International conference on brain informatics. Springer, pp 413–422
4. Al Mamun A, Jahangir MUF, Azam S, Kaiser MS, Karim A (2021) A combined framework of interplanetary file system and blockchain to securely manage electronic medical records. In: Proceedings of international conference on trends in computational and cognitive engineering. Springer, pp 501–511
5. Asif-Ur-Rahman M et al (2018) Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. IEEE Internet Things J 6(3):4049–4062
6. Azmoodeh A, Dehghantanha A, Choo KKR (2018) Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. IEEE Trans Actions Sustain Comput 4(1):88–95
7. Banerjee S, Chakraborty C, Chatterjee S (2019) A survey on IOT based traffic control and prediction mechanism. In: Internet of things and big data analytics for smart generation. Springer, pp 53–75
8. Bertot JC, Jaeger PT, Grimes JM (2010) Using ICTS to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. Gov Inf Q 27(3):264–271
9. Bhattacharya S, Banerjee S, Chakraborty C (2019) IoT-based smart transportation system under real-time environment. Big Data-Enabled Internet Things pp 353–372
10. Bhattacharya S, Banerjee S, Chakraborty C IoT-based smart transportation system under real-time environment. Big data-enabled internet of things. Publisher: IET Digital Library, pp 353–372
11. Biswas S, Akhter T, Kaiser M, Mamun S et al. (2014) Cloud based healthcare application architecture and electronic medical record mining: an integrated approach to improve healthcare system. In: 2014 ICCIT. IEEE, pp 286–291
12. Cadwalladr C, Graham-Harrison E (2018) Revealed: 50 million facebook profiles harvested for Cambridge analytica in major data breach. The Guardian 17:22
13. Chakraborty C, Gupta B, Ghosh SK (2013) A review on telemedicine based WBAN framework for patient monitoring. Telemed e-Health 19(8):619–626. https://doi.org/10.1089/tmj.2012.0215. https://www.liebertpub.com
14. Chakraborty C, Gupta B, Ghosh SK (2013) A review on telemedicine-based WBAN framework for patient monitoring. Telemed J E-Health Off J Am Telemed Assoc 19(8). https://doi.org/10.1089/tmj.2012.0215
15. Chatterjee B, Das D, Maity S, Sen S (2018) Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning. IEEE Internet Things J 6(1):388–398
16. Das R, Gadre A, Zhang S, Kumar S, Moura JM (2018) A deep learning approach to iot authentication. In: 2018 IEEE international conference on communications (ICC). IEEE, pp 1–6
17. Esmalifalak M, Liu L, Nguyen N, Zheng R, Han Z (2014) Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst J 11(3):1644–1652
18. Farhin F, Kaiser MS, Mahmud M (2021) Secured smart healthcare system: Blockchain and bayesian inference based approach. In: Proceedings of international conference on trends in computational and cognitive engineering. Springer, pp 455–465
19. Garg L, Chukwu E, Nasser N, Chakraborty C, Garg G (2020) Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access 8:159402–159414. https://doi.org/10.1109/ACCESS.2020.3020513
20. HaddadPajouh H, Dehghantanha A, Khayami R, Choo KKR (2018) A deep recurrent neural network based approach for internet of things malware threat hunting. Futur Gener Comput Syst 85:88–96

21. Hafeez I, Ding AY, Antikainen M, Tarkoma S (2018) Real-time iot device activity detection in edge networks. In: International conference on network and system security. Springer, pp 221–236
22. Hammi B, Khatoun R, Zeadally S, Fayad A, Khoukhi L (2017) Iot technologies for smart cities. IET Netw 7(1):1–13
23. Harrison C, Donnelly IA (2011) A theory of smart cities. In: Proceedings of the 55th annual meeting of the ISSS-2011, Hull, UK
24. Hashem IAT et al (2016) The role of big data in smart city. Int J Inf Manage 36(5):748–758
25. Hou W, Ning Z, Guo L (2018) Green survivable collaborative edge computing in smart cities. IEEE Trans Indus Inf 14(4):1594–1605
26. Kaiser MS et al (2021) iworksafe: Towards healthy workplaces during covid-19 with an intelligent phealth app for industrial settings. IEEE Access 9:13814–13828. https://doi.org/10.1109/ACCESS.2021.3050193
27. Kaiser MS, Al Mamun S, Mahmud M, Tania MH (2020) Healthcare robots to combat covid-19. In: COVID-19: prediction, decision-making, and its impacts. Springer, pp 83–97
28. Kaiser MS et al. (2021) 6G access network for intelligent internet of healthcare things: opportunity, challenges, and research directions. In: Proceedings of international conference on trends in computational and cognitive engineering. Springer, pp 317–328
29. Kaiser MS et al (2017) Advances in crowd analysis for urban applications through urban event detection. IEEE Trans ITS 19(10):3092–3112
30. Kaivonen S, Ngai ECH (2020) Real-time air pollution monitoring with sensors on city bus. Digital Commun Netw 6(1):23–30
31. Khan Z, Kiani SL (2021) A cloud-based architecture for citizen services in smart cities. In: 2012 IEEE fifth international conference on utility and cloud computing. IEEE, pp 315–320
32. Khanam S et al. (2014) Improvement of rfid tag detection using smart antenna for tag based school monitoring system. In: 2014 ICEEICT. IEEE, pp 1–6
33. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) Ddos in the iot: Mirai and other botnets. Computer 50(7):80–84
34. Li X, Jiang P, Chen T, Luo X, Wen Q (2020) A survey on the security of blockchain systems. Future Gener Comput Syst 107:841–853
35. Mahmud M, Kaiser MS, Hussain A, Vassanelli S (2018) Applications of deep learning and reinforcement learning to biological data. IEEE Trans Neural Netw Learn Syst 29(6):2063–2079. https://doi.org/10.1109/TNNLS.2018.2790388
36. Mahmud M, Kaiser MS (2020) Machine learning in fighting pandemics: a covid-19 case study. In: COVID-19: prediction, decision-making, and its impacts. Springer, pp 77–81
37. Mahmud M, Kaiser MS, McGinnity TM, Hussain A (2020) Deep learning in mining biological data. Cognitive Comput 1–33
38. Mahmud M et al (2018) A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications. Cognitive Comput 10(5):864–873
39. Ozay M et al (2015) Machine learning methods for attack detection in the smart grid. IEEE Trans Neural Netw Learn Syst 27(8):1773–1786
40. Rahman S, Al Mamun S, Ahmed MU, Kaiser MS (2016) Phy/mac layer attack detection system using neuro-fuzzy algorithm for iot network. In: 2016 ICEEOT. IEEE, pp 2531–2536
41. Rathore S, Park JH (2018) Semi-supervised learning based distributed attack detection framework for iot. Appl Soft Comput 72:79–89
42. Rehmani MH, Davy A, Jennings B, Assi C (2019) Software defined networks-based smart grid communication: a comprehensive survey. IEEE Commun Surv Tutor 21(3):2637–2670
43. Saeed A, Ahmadinia A, Javed A, Larijani H (2016) Intelligent intrusion detection in low-power iots. ACM Trans Internet Technol (TOIT) 16(4):1–25
44. Security I (2020) Cost of a data breach report 2020. IBM. https://www.ibm.com/security/digital-assets/cost-data-breach-report/
45. Shafiq M, Tian Z, Sun Y, Du X, Guizani M (2020) Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city. Futur Gener Comput Syst 107:433–442

46. Shakeel PM, Baskar S, Dhulipala VS, Mishra S, Jaber MM (2018) Maintaining security and privacy in health care system using learning based deep-q-networks. J Med Syst 42(10):1–10
47. Sinaeepourfard A, Garcia J, Masip-Bruin X, Marın-Tordera E, Cirera J, Grau G, Casaus F (2016) Estimating smart city sensors data generation. In: 2016 mediterranean ad hoc networking workshop (Med-Hoc-Net). IEEE, pp 1–8
48. Srivastava S, Bisht A, Narayan N (2017) Safety and security in smart cities using artificial intelligence—a review. In: 2017 7th international conference on cloud computing, data science & engineering-confluence. IEEE, pp 130–133
49. Sumi AI et al. (2018) fassert: a fuzzy assistive system for children with autism using internet of things. In: International conference on brain informatics. Springer, pp 403–412
50. Sundararajan A (2017) The sharing economy: the end of employment and the rise of crowd-based capitalism. Mit Press
51. Tomovic S, Yoshigoe K, Maljevic I, Radusinovic I (2017) Software-defined fog net- work architecture for iot. Wireless Pers Commun 92(1):181–196
52. Tyagi AK (2019) Building a smart and sustainable environment using internet of things. In: Proceedings of international conference on sustainable computing in science, technology and management (SUSCOM). Amity University Rajasthan, Jaipur, India
53. Viegas E, Santin A, Oliveira L, Franca A, Jasinski R, Pedroni V (2018) A reliable and energy-efficient classifier combination scheme for intrusion detection in embedded systems. Comput Secur 78:16–32
54. Wang J, Zhang L, Zhang D, Li K (2012) An adaptive longitudinal driving assistance system based on driver characteristics. IEEE Trans Intell Transp Syst 14(1):1–12
55. Ye J, Cheng X, Zhu J, Feng L, Song L (2018) A ddos attack detection method based on svm in software defined network. Secur Commun Netw 2018
56. Zhou W, Yu B (2018) A cloud-assisted malware detection and suppression framework for wireless multimedia system in iot based on dynamic differential game. China Commun 15(2):209–223