**ORIGINAL RESEARCH**

# Contactless Technologies for Smart Cities: Big Data, IoT, and Cloud Infrastructures

Arunmozhi Manimuthu[1] · Venugopal Dharshini[2] · Ioannis Zografopoulos[3] · M. K. Priyan[4] · Charalambos Konstantinou[3]

## Abstract

Intelligent systems are enhancing city environments and improving their overall performance in all possible aspects. Innovations in the field of information and communication technologies (ICT) and the proliferation of big data, internet-of-things (IoT), and cloud (BIC) infrastructures revolutionize the existing agile city ecosystems while effectively addressing customers and citizens needs. In this paper, we address the technology-driven applications that are capable of influencing the existing city infrastructures during their transformation towards smart cities with contactless technologies. We present applications, design principles, technology standards, and cost-effective techniques that leverage BIC for contactless applications and discuss user interfaces deployed in smart city environments. We further discuss state-of-the-art sensing methods and smart applications that support cities with smart contactless features. Finally, a case study is reported on how BIC can assist in efficiently handling and managing emergency situations such as the COVID-19 pandemic.

**Keywords** Contactless technologies · Big data · Internet-of-things · Cloud · Smart city · COVID-19

This article is part of the topical collection "Technologies and Components for Smart Cities" guest edited by Himanshu Thapliyal, Saraju P. Mohanty, Srinivas Katkoori and Kailash Chandra Ray.

✉ Charalambos Konstantinou
charalambos.konstantinou@kaust.edu.sa

Arunmozhi Manimuthu
arunmozhi.m@ntu.edu.sg

Venugopal Dharshini
aishuveu.7@gmail.com

Ioannis Zografopoulos
ioannis.zografopoulos@kaust.edu.sa

M. K. Priyan
mkpriyan@khu.ac.kr

[1] Energy Research Institute (ERI@N), Nanyang Technological University, Singapore, Singapore

[2] APTECH Solutions PVT LTD, Bangalore, India

[3] Division of Computer, Electrical and Mathematical Sciences and Engineering, King Abdullah University of Science and Technology (KAUST), Thuwal 23955, Saudi Arabia

[4] Department of Computer Engineering, Kyung Hee University, Seoul, South Korea

## Introduction

According to a computational and statistical data survey performed by the United Nations Department of Economic and Social Affairs (UN DESA) [1], by 2050, more the 68% of the world population will migrate to urban areas. Typical reasons justifying this transition include the search for improved living conditions, modern facilities and lifestyle, as well as smart and connected assets (e.g., housing units, vehicles, cities, etc.) [2]. However, this rapid population shift towards urban environments can potentially increase the risk of pollution, flash flooding events, lack of housing infrastructure, or evoke other social consequences affecting the citizen's livelihood. To mitigate such threats, scientists and government experts introduced the "smart city" concept. The definition of a smart city is not limited to technological advancements and innovations incorporated into the traditional city infrastructure, but also entails consumer involvement. A *smart city* is an architectural design that can support the economic growth of societies and provide better prospects for citizens—with high standards of sustainability and mobility—leveraging artificial intelligence [3], machine learning [4, 5], robotics, and automation schemes [3, 6].

Technological innovations endorsed the transition towards smart city deployments. Harnessing the advancements in scientific fields such as big data, Internet-of-things (IoT), and cloud technologies (BIC), can assist cities become secure, economically efficient, and sustainable infrastructures, while addressing most of the arising urbanization challenges. Apart from the aforementioned, contactless technology (CT) has recently received great adoption due to its practical and secure way for completing transactions [6–8]. Recently, the COVID-19 pandemic accelerated the need for CT in smart cities. CT has been in use for almost a decade in applications involving smart gadgets and embedded chip-based tools used for contactless payments, identity verification, attendance monitoring, etc. In early 2000, magnetic strip-based payments were used in banking systems, and later on, CT payment methods were introduced through which users could make payments at dedicated embedded devices. Over the past few months and given the COVID-19 outburst, a massive digital transformation has occurred, forcing companies to adapt to the new circumstances. In more details, almost 68% of enterprises have turned to digital technologies to retain their customer base, service provisioning and with minimum impact on the enterprise operation. Notably, during the pandemic global crisis, technology-driven smart applications including IoT devices (e.g., smartphones, computers, smart watches, and sensors) improved the security and safety of citizens while keeping them socially isolated from the outside world to disrupt the virus spread per the government safety regulations.

A field study from the World Health Organization (WHO) and the United Nations predicts that there will be a 40–75% increase in technology-driven startups by 2030, which will be addressing the socio-environmental challenges around the world. Smart cities can furnish technological innovations improving the sustainability and living quality of urban environments. Different information and communication technologies (ICT) technologies assisting this digitization thrust along with their functional capabilities and resource requirements in different sectors are illustrated in Fig. 1.

Consumer engagement, business objectives, and application interfaces motivated the shift towards CTs which can positively influence smart ecosystems, making them environmentally friendlier (e.g., by reducing the use of paper for documents, plastic for cards, etc.). Different use cases and application-specific fields encountered within smart city deployments (e.g., mobility, energy, healthcare, etc.) can be leveraged for the design, development, and evaluation of contemporary technologies enabled by BIC. Smart cities
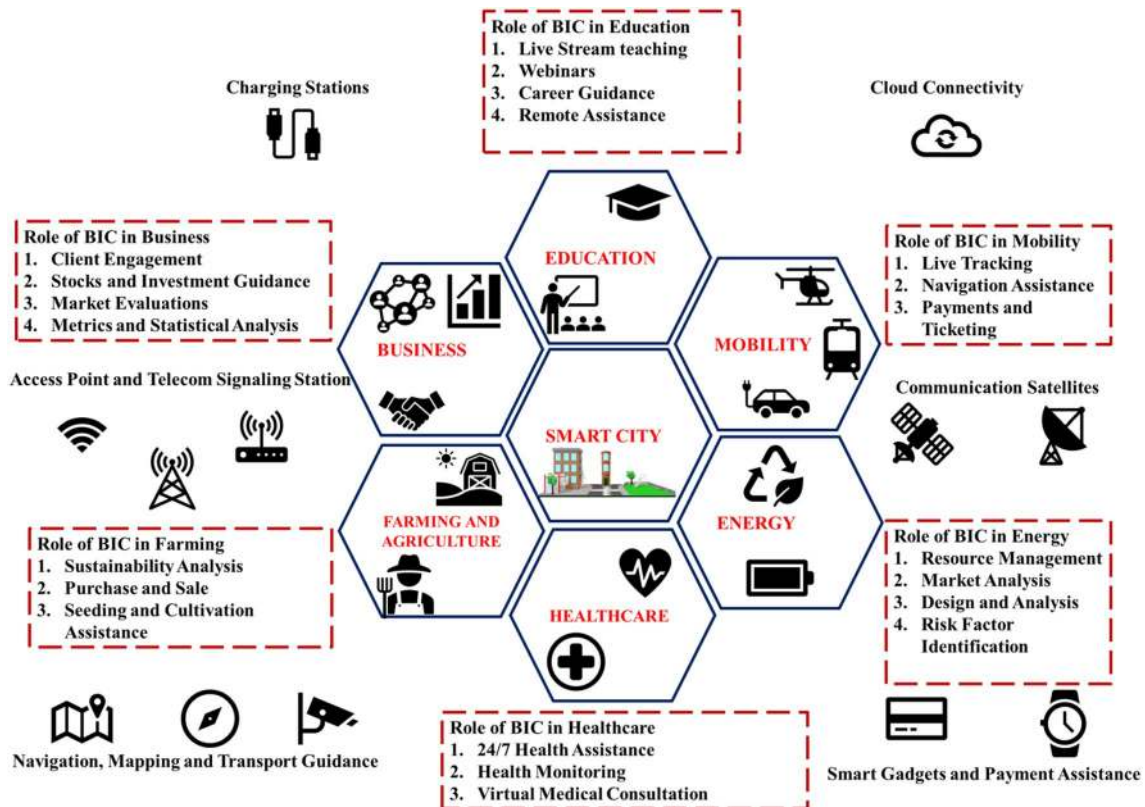


**Fig. 1** Overview of the information and communication technologies (ICT) within smart cities assisted by big data, Internet-of-things (IoT), and cloud (BIC) infrastructure

equipped with CT gateways can support high growth rates, become more competitive, and attain bigger market capitals when compared to business entities operating using outdated tools. COVID-19 has demonstrated the effectiveness of CT for different applications and paved the way for even some rural areas which tested BIC-enabled techniques, mainly in industry-based applications, proving their cost-effectiveness. Depending on the actual environment, where such CT are are employed, for instance in construction, transportation, business models, consumer engagement policies, etc., they can furnish a plethora of additional features [9].

The key contribution of this paper is to showcase the increasing number of CT applications within smart cities that can be promoted by BIC. A field study as well as a forecasted statistical analysis about BIC in their individual domains are briefly presented in Sect. 2. Detailed case studies, related literature, and the impact of ICT in smart cities are discussed in Section "Related Work" to raise the readers' awareness regarding the benefits of CT. The inter-relationship between BIC and application-specific innovations for CT are explained in Section "Contactless Technology (CT)". Different technologies and their actual/forecasted impact on societal implications from the smart city's perspective are also explained. Cross-platform technologies, applications, and technologies driving CT towards smart ecosystems in smart cities are discussed in Section "CT in Smart City". The impact of big data in healthcare, national security, and various surveillance schemes is detailed in Section "Big Data Biometric Analytics: A CT Paradigm". The importance of IoT for autonomous vehicles (AV) is examined in Section "IoT in Autonomous Vehicles (AV)". Furthermore, given that cloud-based infrastructures are increasingly used in many embedded applications, the relation between contactless payments and cloud-based requirements are explained in Section "Frictionless Payment Technology and Cloud Infrastructure". A case study about the impact of BIC for smart cities in India during COVID-19 is presented in Section "Contactless Payments with NFC". The security and safety standards which should be mandated before the deployment of CT in the smart city ecosystems are introduced in Section "A Case Study of Utilizing BIC Technologies During COVID-19". Finally, Sections "Discussion on the Implications of Utilizing BIC", "Conclusion" delineate the implications of CT and conclude with directions for future work on this topic.

## Related Work

Smart city technological transformations require significant investments [10], innovations [11], research plans and long-term infrastructure analyses [12]. Numerous venture capital investors, business analysts, and government agencies

should actively participate in the development of the complete city infrastructure provisioning smart features to citizens. If comprehensive studies are not performed and strict deployment plans are not respected, urbanization can lead to unstable economic growth and negatively impact the smart city transition on a global scale. Typical challenges include generation, transportation, and distribution of power, water supply, connectivity, and communication [13], healthcare [14], schools and colleges, etc. Rapid urbanization has also affected the agriculture sector too. Technological innovation, careful planning, and management of operations are critical requirements to conserve the existing infrastructure and materialize smart city schemes [15, 16].

About 36% of the developed countries already implement smart city concepts within their borders. Countries like India, China, Japan, Bangladesh, Myanmar, and Indonesia have successfully built their smart city infrastructure, accounting for almost 27% of the world's population [2]. A lot of opportunities, challenges, and critical factors have been analyzed during the design and planning phases granted that each smart city project could approximately cost around 25–30 million USD. With such considerable investments, ICT play a vital part in the implementation and deployment of smart city concepts. ICTs can ensure environmental sustainability, integrate technological advancements, and assist in balancing economic growth without inhibiting the transition towards smart city ecosystems. Notably, statistical analyses shows that in 2000, only 15% of the world population was living in cities, whereas, in 2020, almost 50% of the population has moved to urban environments, ad by extension smart cities. Furthermore, according to the United Nation's analysis, by 2050 almost 70% of the population will be located in complete smart city deployments and nearly 80% of the rural areas will have been urbanized incorporating technological innovations and scientific advancements [17].

Every year, about 7–12 projects affecting population units in the range of 30–50 million people, and generating revenues in the vicinity of 10–12 billion USD will be executed in most developing nations. Government agencies and policymakers are endorsing the urbanization in combination with the transition to smart cities, leveraging ICT and other current technological developments [18, 19]. Designing a smart city plan harnessing ICT and BIC is a daunting task due to the security requirements that need to support and protect the interoperable infrastructure web. In the smart city domain, the physical world communicates using embedded devices, software and numerous computational algorithms that provision better quality of service for the consumers. The contribution of the 3rd generation of internet—in the early 1990s—had a significant impact on the development of the 6th generation (6G) internet technologies that are utilized today. Interconnected networks, smart communication

standards, large amount of big data exchanges, etc. provide seamless service integration, improve application interfaces as well as the user quality of living. Nearly two thirds of the available devices in smart cities are wireless, which illustrates the communication synergies that can be implemented for diverse applications and at large scale.

Once the system design is established (comprised of multiple embedded devices serving as autonomous agents), security and safety are major concerns when managing, storing, computing, and analyzing user data [9, 20]. Thus, ICTs must employ smart security schemes ensuring the confidentiality of the data residing in the mentioned devices. In 2009, the world's 1st smart city in Santander, Spain had around 20,000 decentralized sensors ,which were distributed throughout the urban landscape, collecting and transferring user information. Initially, during the transformation from offline processing and analysis to digitization with smart computerized processing, analyst and technical people finds it a bit difficult due to their high-speed processing capabilities and result oriented computations [4, 13]. Later stages of data processing made them clear that there is no manual analysis and process re-verification is necessary due to their encryption-based complex algorithms.

Decades of advancements in ICT have caused serious impacts on the socio-economic well-being of people living in smart cities. The rapid growth of the internet and communications enabled smart city residents to remain connected to the internet in every aspect of their lives. Thus, IoT became an inseparable element of every smart community. Many researchers [7, 21, 22] surveyed the impact of IoT in smart city expansion. Focus on urban IoT scenarios with their application-specific objectives made clear that the transformation to smart cities requires considerable planning and technology-driven testing in real time. IoT can be found in many applications such as traffic systems, healthcare, home and industrial automation, power generation and delivery sectors, and in many customized services aimed at assisting certain demographics. An empirical survey on urban IoT helps identify the intertwined concept of quality and quantity; improving the quality of the living environment in urban IoT infrastructure will also assist the economic growth of the city [4]. During this IoT integration process, the city operational costs are greatly reduced, while the fundamental lifestyle of people improves significantly.

A case study performed in Padova shows that open source data obtained from different sensors and actuators installed in many public areas can be integrated using IoT and used for monitoring the entire city from a centralized government-operated interface. IoT provides a wide range of design options and solutions; however, the security of the devices and the algorithms used should conform to the current cyber-security standards. The authors in [21, 23, 24] present a detailed survey on security issues, challenges, and their

attack mitigation for IoT devices in smart homes. Since data security is handled by the service providers, data confidentiality, resource availability, authorization, and integrity must also be ensured along with non-repudiation. The authors performed an adversarial analysis, where IoT risk factors were analyzed and categorized (in three different groups) based on their severity and economic impacts [25]. Domestic electrification, transportation, and grid integration are the key areas analyzed in the survey along with potential countermeasures. In such smart IoT setups, enormous amounts of data are generated from multiple sensor and embedded devices, thus proper attack categorization and comprehensive security analyses are necessary to ensure data security [26, 27].

The need for efficient big data management becomes vital due to the inherent advantages that can provide to users and enterprises. Big data analysis can offer automatic suggestions and user-friendly choices for consumers, and can also be employed in various other industries, such as e-commerce, transportation, health and medical field, and education. The collected data have to be processed and stored before computations can be executed and useful results are generated. Big data privacy protection mechanisms are leveraged to safeguard customer data [20] . Encryption tools, privacy-preserving computation models, complex data management algorithms are required to preserve the confidentiality of user-generated data (stored in government databases) for further analysis and processing. Networking standards should also conform to security recommendations and best practises when handling sensitive user data, promoting trust, and assisting in building secure connected communities.

In 2015, United States (U.S.) Networking and Information Technology Research and Development (NITRD) program released a framework for smart infrastructure communication zones which includes IoT-BIC and envisioned the development of completely autonomous cyber-physical connected smart community (CPSC) [3]. This CPSC would possess networking units, communication devices, big data stack, decision-making models, and high-fidelity cloud-assisted real-time assistance systems. With the complete smart infrastructure, industries and power distribution units will also be easily accessible, while the traffic management systems would become more eco-friendly. To avoid data congestion from the embedded agents, all seven distinct components must be collectively controlled and maintained [28].

Services that run in the background and can overcome potential abnormal conditions should be designed to maintain safety and security while complying with the international standards organization (ISO) regulations [29]. Although big data management may endorse the growth of smart cities the user accessibility to resources in such ecosystems can become a challenging task. To ensure user access to the available resources, cloud infrastructure

must be enabled in these smart communities. This cloud-assisted data collection, resource management, and application processing can help users get their desired results promptly. From banking and parking payments to other applications like billings, medical records, driving assistance, etc., data can be stored in the cloud and can be instantly delivered to the authorized users. These cloud databases require sophisticated big data management schemes and robust IoT connectivity mechanism for seamless data communications. During the last few decades, cloud service providers like Google, Microsoft, and other e-commerce industries have been utilizing both private and public cloud infrastructures assisting real-time applications [17, 30]. The mentioned cloud services requires substantial internet-connected resources and large data storage facilities for the collection, processing, and analysis of the aggregated data. As a result, in smart communities the three essential components, i.e., BIC, must be leveraged and secured for long-term sustainable economic growth and user-friendly ecosystems.

## Contactless Technology (CT)

With the advent of COVID-19, CT, or Touchless Technologies have become the new normal. The pandemic uncertainty has affected everyone around the world. The need for innovations and new technologies has been increasingly requiring for more human and artificial intelligence (AI) collaboration. Organizations are already adopting new concepts using AI, robotic process automation (RPI), cloud-based systems, and other automation technologies to promote their business and combat the pandemic-induced impacts [30, 31].

Technologies like big data, IoT, AI, radio-frequency identification (RFID), near-field communication (NFC), machine to machine (M2M), MIkron FARE Collection System (MiFare)/DESFire RFID reader, etc. are few of the CTs assisting people. Thus, BIC schemes must be investigated before their adoption in more future applications. The mentioned CT can create opportunities for scientific advancements, improve task proficiency, and provide profitability benefits [8]. AI leverages human intelligence concepts to allow machines execute complicated tasks, IoT consists of interconnected physical devices featuring sensors, using software, and other wired or wireless technologies, and big data consists of complex and extremely large data sets generated from consumer devices, industrial components, automobiles, etc. Consequently, BIC technology works in an orchestrated manner leading to many innovations [21, 32,

33]. The connecting links between these three technologies are given below.

## Big Data and Cloud Computing

Cloud assisted data analytics are crucial for the constantly growing data-centric era. For every instant that passes, large amounts of data are generated from embedded mobile devices, electronic gadgets, and computing resources. Such data are stored in local servers if instant access is required, while confidential data are stored in secured private cloud databases utilizing essential safety and security countermeasures. The data can be retrieved or accessed from remote locations by authorized users leveraging the appropriate remote connection frameworks [15, 20, 34]. Thus, a suitable big data analytics tools are necessary for the management and effective handling of cloud data introducing the need for analytics as a service (AaaS) platforms.

Multiple licensed cloud service providers like AWS, TensorFlow, Hadoop, and private data analytic cloud-based ventures provide customized application programming interfaces (API) for their users depending on their needs. Private companies involved in this field provide 24/7 network assistance to their consumers. Typical examples of applications and user groups requiring data assistance services and/or remote cloud support are demonstrated in Fig. 2. Other trust-based cloud service providers also exist for applications including government databases, military, and national security purposes, etc. [29]. Such features illustrate the advantages of cloud-based big data analytics, emphasize their importance, and present the diverse usages of cloud infrastructures.

## IoT and Big Data

IoT can capture and process data from electronic devices and machines, process them while making them accessible from any remote location. However, for such applications, authorization, user verification, and security protocols have to be followed. Upon gaining permission and accessibility from individuals through their IoT enabled devices, the interactions between M2M can be analyzed and studied. This data-centric approach of IoT-big data helps categorize user behavioral patterns and assist them with tailor-made results meeting their requirements in real-time [21, 35]. IoT capabilities can also be enhanced employing AI methods allowing for hyper-realistic M2M interactions mimicking human behavior. AI algorithms with their wide range of applications can enhance the user experience when handling IoT devices and provide additional custom functionality—based on the user profile—when dealing with big data.
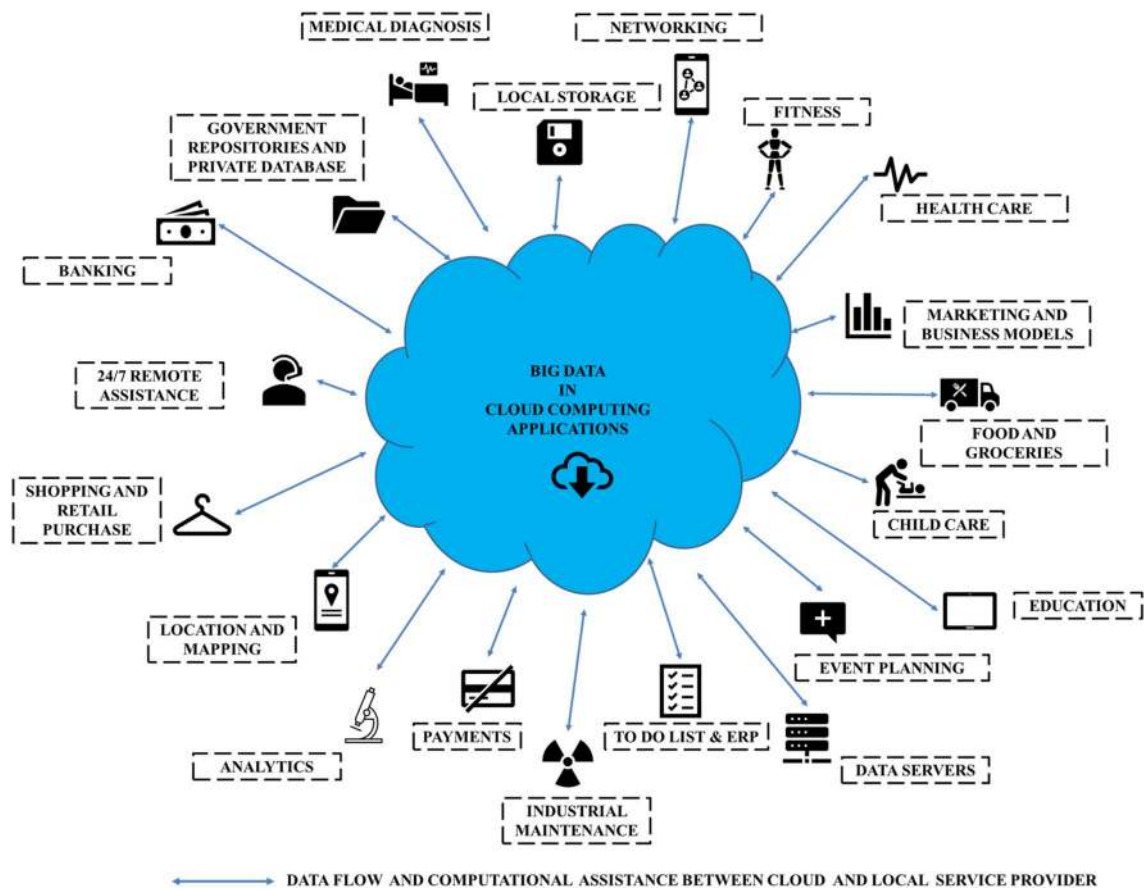
**Fig. 2** Application areas of big data in cloud computing

## CT in Smart City

Touchless technology is a promising way to maintain people's health and hygiene, especially during crisis such as the COVID-19 outbreak. A recent survey reports that due to the COVID-19 pandemic about 95% of the people prefer touchless services like touch-free alcohol or soap dispensers, touch-free faucets, etc. Contactless or touch-free technologies can be leveraged for different products and services. Some contactless technologies that can promote smart cities infrastructures are discussed in the following sections.

## Touchless Biometric Solutions for Access Control

Fingerprints, iris, and face recognition are the biometrics elements used for identity, temperature sensing, and access control in many organizations. To reduce the risk of disease spreading in workspaces, a Swiss-based company named touchless biometric solution (TBS) has emerged offering two services, the TBS 2D Eye and the 3D Terminal.

### 2D Eye System

Serves as a combination between two techniques, i.e., the iris scanning and the face detection, reaching accuracy levels of 95% and enhancing the security of access points. The process starts with facial identification through images captured using a highly sensitive camera. Then, iris details are extracted from the images and analysed for the user authentication [2, 36].

### 3D Touchless Fingerprint Scanner

Provides an even higher level of security, recognition performance, and authentication accuracy (compared to the 2D Eye System). The 3D touchless system achieves authentication accuracy of 97%, while only 5–8 ms are necessary for the extraction of the fingerprint scan. Furthermore, the 3D touchless system is resilient against light beams, UV and IR laser pointers and can withstand exposure to dirt, dust, smoke, and fog [7]. The entire module is resistant to abusive treatment involving contact or contactless use, while its sensitivity level remains high allowing for correct authentications even if the person wears surgical gloves or any other

industry-grade latex gloves that are used in hospitals and chemical laboratories.

Both 2D and 3D scanning systems have now been updated to include additional security features which can assess the user's emotions and measure the body temperature when the TBS system scans the person. If abnormal body temperature is registered, TBS will not authorize the user. Similarly, gesture controls have also been included to mitigate the use of sign language and physical movements from end-users. The COVID-19 outbreak has increased the demand for CT; thus TBS can help companies provide safer working environments for their employees [22, 30].
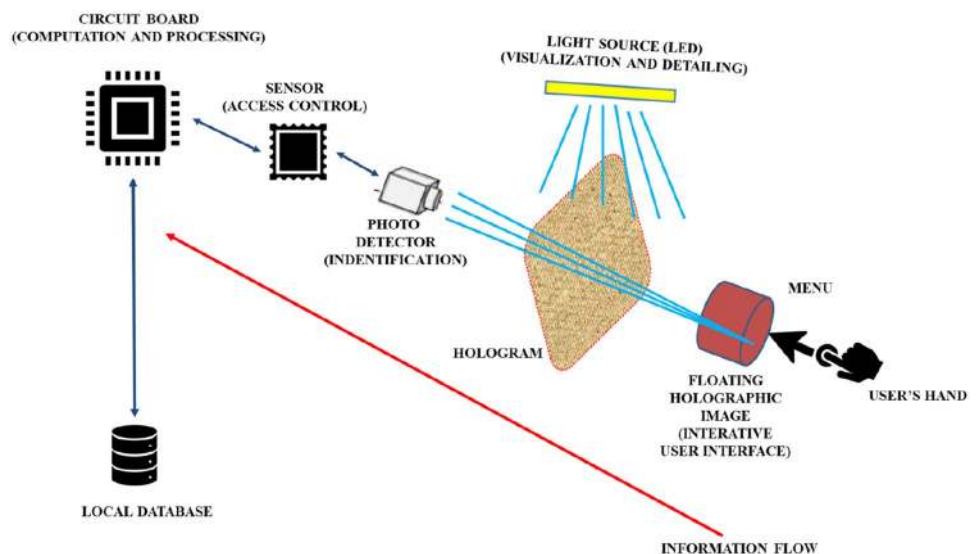
### Thermal Scanner Systems/Temperature Detecting Cameras

Both schemes use thermal sensor modules to identify the body temperature of an individual and alert them if their body temperature is outside the nominal level. Touchless biometrics have been utilized in the healthcare sector too. Body area networks (BAN), wireless body area networks (WBAN), body sensor networks (BSN), or medical body area networks can assist in comprehensive healthcare monitoring by monitoring body vital processes and tracking patient activities, etc.

### Wearable Bands

Wearable bands are smart electronic devices worn over the surface of the skin, e.g., typically over the wrist. They analyze basic information like body blood pressure, heart rate, oxygen saturation, etc. and can also track activities (walking, running, sleeping, etc.). Apple smartwatches, Fitbit, Garmin, Suunto, Polar products, etc. are some of the most commonly used wearable devices available in the market.

### HoloTouch

This technology uses human-machine interface (HMI) and works by allowing people to pass their finger through holographic images or buttons or keyboards which are floating in the air. Then, an infrared sensor detects and transmits the measurement to the detection software as shown in Fig. 3. Other similar applications to Holotouch include optical computers, biomedical imaging, scanning and diagnosis, and destructive or non-destructive testing in military applications. Some of the applications of HoloTouch have been used in China for touchless holographic elevators, hotels and room sections, or for food orders and payments.

### Voice Recognition and Virtual Assistants

This technology works by collecting voice samples as input from the user and then decode them with the help of natural language generation (NLG). In addition, the voice recognition units as well as other CT like biometrics, face detection, HoloTouch devices, etc. can be used to perform a plethora of tasks as demonstrated in Fig. 4.

## Big Data Biometric Analytics: A CT Paradigm

Big data biometric analytics is a technique, where personal data from the consumers are collected, processed, and analyzed for numerous reasons. This combinational was used even further during COVID-19, since contactless operations were implemented in many corporate settings. Furthermore, many industrial units mandated the use of biometric methods to grant employees access to the workplace. A recent survey from the Forbes magazinereported that the Indian government has implemented the unique identification authority of

**Fig. 3** Overview of the Holo-Touch setup

**Fig. 4** Overview of smart contactless applications



India (UIDAI) which aims to manage and maintain India's Aadhaar citizen registry [20, 37]. The key factor in Aadhaar is the collection of personal information from citizens. Such information include iris retinal scans, fingerprints, residential addresses, and digital face registrations. All these are clustered and maintained by MapR, an enterprise-grade NoSQL database in Hadoop. MapR is used due to its high-speed data verification performance, i.e., within 200 ms, 3–5 MB of individual data are obtained from people, processed and mapped to the database to get the exact evaluation results. This software-based data entity works on the Hadoop platform and uses big data analytical algorithms for the processing and analysis [37]. To obtain meaningful outcomes from the captured data, large and complex programs were developed. These algorithms evaluate the consumer personal data both statistically and visually depending on the requirements, thus parallel computing is crucial for this scenario. Big data programs have the potential for parallel computing and data visualization, making the analytical framework easily interpretable by all domestic consumer entities upon proper government approval. The proliferation of contactless consumer electronics that use image recognition software, sensor-based encryption, and pattern mode decoding require big data storage infrastructures and processing power for essential computations.

## Contactless Biometrics in Healthcare

COVID-19 has a global impact in the health sector affecting 15–20 million people around the world. The pandemic has enforced the use of contactless biometric technology.

Biometrics available in hospitals help identify doctors' availability, patients' health conditions, medications, and aid with resource management and health care professionals' status. Depending on the biometric algorithms used, records about patients, doctors, and other medical workers were stored and retrieved during emergencies. The University of Pittsburgh medical centre (UPMC) has developed a fully operational biometric system enhancing the patient's user interface [12, 38, 39]. The developed system was installed in around 75 cities with 4300 biometric devices for the recording of user data. The recorded data can help the government keep track of the citizens' socio-welfare behaviors and medical conditions. More personalized functions such as voice assistance and iris scan assistance can help people during emergency situations. Recording patients' records into a common database ensures a centralized tracking mechanism of their health condition. Hospital management can benefit from such systems as long as they are interested to make this one-time investment. Record creation and maintenance, analysis and medication, treatments and procedures, summary reports and billing, etc. can be retrieved from the common biometric-enabled contactless big data database [40, 41]. Furthermore, some specialized healthcare establishments in the United States could even store the patient's DNA data along with other biometric features. DNA Records can help trace the patients' identity in situations such as accidents, murders, or other potential crime scene investigations.

This DNA identification feature in combination with CT promotes the use of big data algorithms for applications such as health monitoring and user tracking leveraging smart

wearable devices. User data is mapped with their existing health records and this can help track their current conditions, localize them during emergencies, etc. To underline the practicality provided by biometric technologies and big data analytics, we consider an Indian hospital scenario. The Apollo hospital was established in 1983 and has successfully achieved many advanced scientific breakthroughs in the medical sector. The success of Apollo hospital relies heavily on big data and biometric functions. For instance, the hospital is using the *Askapollo* application, which is an Online appointment scheduler to streamline the management of its patients [17, 42]. The virtual scheduler can help the patients or any user book appointments for normal health check-ups, doctor consultations, or any other medical services, e.g., X-rays, etc. If a patient registered with the Apollo hospital faces an emergency, the patient's record will be sourced from the hospital's database to expedite medical procedures. Using this optimized and patient-centric database, people with rare blood groups or people who are willing to donate their organs can be effectively tracked during emergencies. In addition, one-to-one doctor-patient consultation (via video) is also provided for the registered hospital patients. During such consultations, the patients' records are revoked from the Apollo database, including case sheets, medical conditions and medications, and other relevant that can help doctors conduct their diagnosis. The practicality of this feature was emphasized during the COVID-19 crisis, since patients were able to reach their doctors without jeopardizing their health (e.g., if they had to visit the hospital in-person) [42].

In the healthcare environment, touchless technologies can assist in preventing the cross-contamination of hospital facilities. Aspects such as hygiene, safety, and accessibility are of great importance for the healthcare sector. To overcome potential issues, the Yale New Haven hospital (YNHH) has installed touchless holographic switches, replacing traditional tactile switches. The touchless holographic switch is operated by passing a finger through a holographic image that is floating in the air in front of the switch's bezel. Unlike tactile switches, the touchless switches do not need to be physically touched. Such technologies allow people to intuitively enter commands by simply accessing a virtually displayed hologram image, which could be in the form of keys or buttons or PIN projected from an embedded holographic signal emitter. Light detectors, using optical or infrared beams can capture, classify, and diagnose the selected keys and transmit them to the embedded processing unit for analysis [42, 43].

## Biometrics in National Security

Contactless biometric techniques are also employed by National Security organizations around the world. Many countries have already implemented such schemes since 2014 in their government facilities and during the COVID-19 crisis, contact tracing, entrance/exit systems, immigration, and medical records were all operating using biometric verification and analysis. In more detail, some countries have implemented strict border control and immigration rules to protect their citizens and inhibit the virus spread. In addition, biometric authentication mechanisms have been widely used for the verification of security personnel who work in mission-critical positions (e.g., army, central intelligence, etc.) [43]. The United States has mandated the record retention of military personnel biometrics for identification and verification before granting entrance to the nation's military facilities. Likewise, North Korea has integrated AI features along with biometric and facial recognition software in their homemade smartphone 'Jindallae'. AnyVision, an AI-based security company based in Israel, and supported by Microsoft, has established its business in 40 different countries around the globe. AnyVision builds key-based authentication, identification, and access control systems using custom built API and software development kits. Thus, protecting the privacy leveraging facial recognition, iris scan, and thumb impression mechanism. As a result, confidential data can be accessed by authorized personnel providing reliable and trust-based real-time authentication [44]. Different policies and practices are implemented by countries when handling biometric methods to protect their military infrastructure [13].

As connectivity continues to spread across the globe, the use of touchless technologies is also expanding to more applications. From nuclear warhead management to fighter jet missile launching, soldiers are identified and authorized based on their personal biometrics. Data obtained from sensors in battle tanks are used to analyze the identity and current status of the operating personnel during military missions [45]. Battleship and submarine captains are also authorized only using their personal biometric scans. Thus, with contactless big data biometric strategies, nations can identify potential terrorists and criminals before they arrive on their borders sourcing their criminal records from the national databases [46].

## Biometrics in Airports

Many international airport checks are completely automated, and passengers are granted entry to theory destinations upon their successful biometric verification. Semi-autonomous biometric kiosks are installed at every entrance and exit point, and passengers are advised to use them for identification purposes. This mode of immigration clearance has helped during the COVID-19 crisis [47, 48]. In Singapore for instance, until 2019, there were about 2.16 million immigrants (out of 5.7 million

net population) all of which were given safe entry to their home country after registering with their biometrics at Singapore's database. Passport scanners, face recognition, and thumb impressions were obtained from every passenger during immigration clearance, as shown in Fig. 5. This mode of identification helps protect nations from potential terrorist incidents and during unexpected emergencies such as the COVId-19 outbreak.

In 2015, U.S. Homeland Security implemented biometric services for customs and border patrols. These mechanisms aided security officials in identifying illegal immigrants, trespassers, and terrorists before entering U.S. soil. Data obtained from immigrants were saved in FBI databases and retrieved for future identification [49, 50]. The biometric databases are frequently updated to track immigrant activities as well as short- and long-term visitors under different visa categories.

In 2018, the Bangladesh army organized a biometric registration campaign to deal with the Rohingya refugee problem. The statistical reports demonstrate that Bangladesh is hosting more than one million refugees which is 13% more than the official estimate. Such results where brought to the surface due to the effective use of biometrics collected from native citizens and refugees. Upon obtaining the analysis results, most of the countries belonging to the Association of Southeast Asian Nations (ASEAN) stepped in and offered aid and medical resources to the refugees [51, 52].

## Biometrics in Domestic Surveillance

Domestic surveillance using biometric techniques helps identify, measure, and analyse the people's physical and emotional behaviors. Some of the physical biometric features include fingerprints, DNA samples, and digital photos. In addition, in mission-critical cases, even data concerning a person's voice, tone pitch, and walking patterns can also be used for military database. In 2015, U.S. Homeland Security used facial recognition methods to capture the facial expressions of criminals and this feature proved extremely helpful in recognizing criminals from crime scene surveillance footage. The identification range varied from 40 m to about 200 m and achieved excellent results using facial biometric features. Image processing techniques and big data analytical algorithms greatly helped in this thrust. To analyzing criminals' mindset and decipher their behavior during interrogation and judicial investigations, emotional state-based analysis is also used in many countries [46, 47, 51].

Emotional state-based analysis includes facial expressions, voice, posture, walking pattern, and other schemes for prediction, analysis, cross verification, and exact identification of criminals. In Singapore, in every residential apartment building corridor high fidelity cameras are installed and the whole country is kept under surveillance to mitigate crime. DNA profiling is another trending contactless biometric technique that is already in use by the FBI and Interpol. In more detail, DNA profiling helps identify criminals from their blood samples and palm impression collected
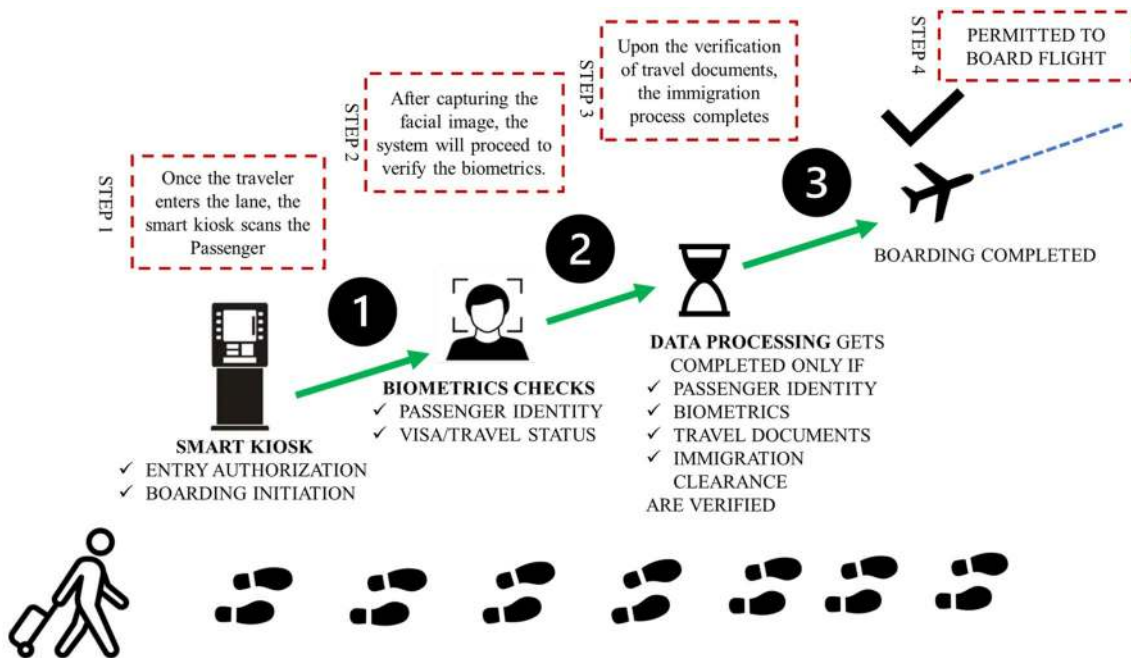


**Fig. 5** BIC processes in airports for passenger identification and document verification

from the crime scene. Recently, Japanese researchers have developed and deployed robots in big malls and crowded public communities to capture people facial patterns. These robots record the emotional activities (fear, stress, smile, joy, etc.) in real-time and map all these data to the country's biometric database [42, 43, 48, 49]. Emotional activity is monitored to understand the mood and mindset of people, while unusual activity will be reported to the nearest police station. Other than criminals tracking, domestic surveillance methods are used to identify vehicle number plates, and in some assisted parking sections, vehicles will be allotted parking spaces based on the passenger details. Such computations using sensitive user data require complex cryptographic algorithms to protect the databases from potential malicious hackers.

Both security and safety go hand in hand with big data biometric contactless techniques paving the way for many other futuristic applications. Ethics and information technology (IT) warn about the vulnerable elements when using biometric features in fields like surveillance, tracking, identification and authorization [3, 29, 38, 44]. Unauthorized use, access limitation,and erroneous classification of features are the pitfalls that require immediate attention when using biometric techniques.

# IoT in Autonomous Vehicles (AV)

Connectivity plays a major role in the synchronized operation of AV. A better understanding of the environment and user behavior is achieved leveraging IoT electronic devices inside the AV. IoT sensors enable self-driving vehicles transitioning from the manually driven vehicles to completely autonomous units. From assisting sensory mechanism and actuators to software-in-loop (SIL), the operation is governed autonomously without any human interventions. Autonomous refers to the self-driving ability of vehicles using smart sensors and actuators. Developments in areas like IoT and machine intelligence, computational capabilities, and real-time decision-making algorithms are leveraged in broader aspects when designing AV. Control circuitry is maintained and modulated based on the commands and driving pattern of the consumers [53, 54]. Remote connectivity using private cloud infrastructure renders the AV sensors constantly connected (in a 24/7 basis) both during the runtime operation as well as off-road during resting periods (e.g., parking, electric vehicle charging, etc.).

Localization, mapping, mobility, and security are completely programmed and controlled by sophisticated electronic elements like LIDAR, RADAR, cameras, etc. Parking assistance and traffic navigation with improved safety for both the user and he pedestrians, fuel and tire pressure monitoring unit, and lot more features are fitted and can be coordinately controlled and monitored from remote places exploiting the IoT.

## Augmented Mobility Assistance

IoT ensures smart and safe operation of AV for both passengers as well as pedestrians with the help of on-board sensors and other embedded components. Data collected from the available sensory elements are connected and communicated via customized private cloud services and are instantly processed remotely for smooth control and operation of the vehicle. Adversarial analysis can be made with IoT-enabled smart sensors for quick recovery from cyber-attacks [55–57]. Data obtained from sensors are used to analyze the passenger's behavior, driving patterns eventually providing a tailor-made driving environment for the users. Some of the key benefits for fitting IoT devices in AV include:

1. Improved road safety and driving assistance.
2. Enhanced traffic navigation and optimal route identification.
3. Smart connected car environment.
4. Better fuel and battery management mechanisms.
5. Driving comfort and better localization.

## IoT Enabled Traffic Navigation

Automakers are working towards completely autonomous driving mechanisms which corresponds to level 5 of the society of automotive engineers (SAE) standards. Granted the multitude of on-board sensors, electronic and communication devices, vehicle location services, user driving pattern recognition mechanisms , vehicle surrounding assessments, etc. autonomous driving cars can be easily monitored and analyzed [7, 10, 32, 57]. Although vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) concepts can become challenging in the dense traffic setups, reliable navigation assistance is possible using high precision sensors and actuator units. Developments in communication standards like 5G and recent advances in public cloud facilities—with enhanced security due to state-of-the-art cryptographic algorithms—IoT-enabled AV navigation can be achieved even during peak traffic periods in urban areas. Figure 6 shows the effect of BIC during AV navigation. All the data are delivered to AVs and assist the vehicle's central controller to perform critical tasks without any additional input or manual assistance from the driver.

## Localization and Mapping

RADAR, LIDAR, and cameras are the key components required for smart localization, mapping, and navigation of AVs. The IoT sensors in these components control and

**Fig. 6** BIC-enabled services for AV transportation and navigation purposes
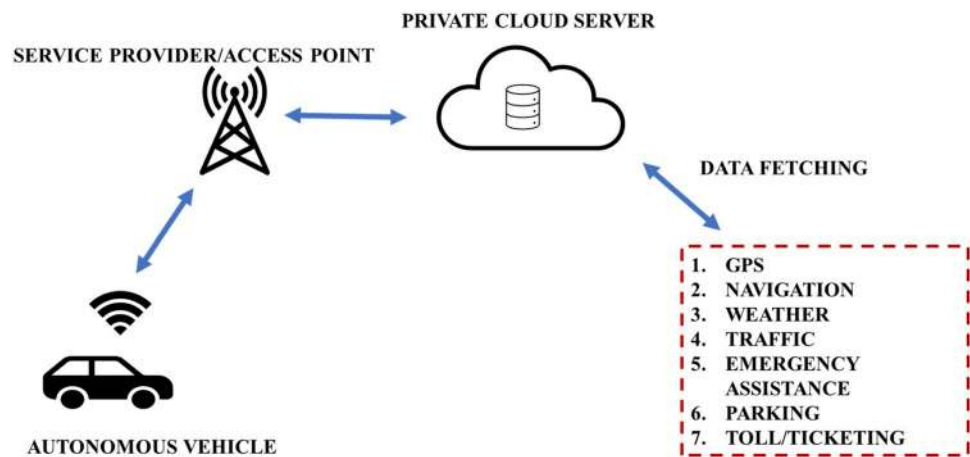


coordinate the operation of AVs. The data obtained from the on-board AV sensors are used for mapping and localization purposes. After the current position of the AV is identified, it can be routed to any location using the aforementioned smart sensors, i.e., cameras, RADAR, and LIDAR. During driving, the embedded sensors manage the engine control, tire pressure, fuel levels, etc. providing a smooth driving experience to the passengers [53, 54].

## IoT in Smart Infotainment Systems

Apart from driving assistance applications, to ensure better passenger experience, embedded features withing the vehicle's infotainment unit collects data about passengers driving pattern and habits (e.g., cabin temperature). Infotainment systems can support a variety of services such as, internet/Wi-fi connectivity, streaming audio and video, voice control and calls,, touch control, and air conditioning unit operation, etc. All these features are enabled by the embedded sensor, which collect data, analyze them, and optimized the vehicle conditions enhancing the passenger experience [41, 58, 59].

## IoT for In-Network Computing and Operations

Sensors and other embedded components deployed in AV perform in real-time numerous computations for navigation and safe driving as well as run high-level security algorithms for user data privacy and protection. High fidelity sensors perform multiple time-critical operations and help AVs in their analysis and decision making procedures under varyin operational conditions, e.g., during peak traffic. These embedded actuation and smart sensing units are programmed to control and coordinate with each in V2V and V2X deployments [60]. IoT-enabled devices deal with different time-critical tasks which can be controlled and monitored from remote locations leveraging cloud-based resources. Automakers equip their recent models with cloud-assisted

driving features improving both their consumer safety and efficiently navigating them to their destinations. The massive amount of real-time data collected and analyzed, within AVs, from their sensors and computation units have to be secured from adversaries. Protecting sensitive user data from malware, spyware, attackers, etc. mandates the use of secure encryption schemes like transport layer security (TLS) 1.3, quantum cryptography among others [23]. All these cryptographic methods should operate in parallel with the data collection (from sensors) and computations performed in the corresponding units maintaining end-user safety and security [24, 61].

## Frictionless Payment Technology and Cloud Infrastructure

Frictionless payment technology is comprised by all the mechanisms and operations that streamline the make the shopping experience for the clients. For instance, Amazon's "just walk out" service is a great example for this technology. It simplifies the buying process, allowing customers to enter, grab the items they need and just leave. The walkout technology keeps a track of what products shoppers add in their virtual carts. Once the shopping is done, their credit card is charged for the items they have purchased and their order receipt is emailed to them automatically [62]. Figure 7 shows the global sales of smart gadgets in various cities around the world. Gadgets whcih can be used for frictionless payments include mobile phones, mobile wallets, contactless cards, and NFC-type devices, etc. [2, 63].

It is estimated that the value of ICT will grow 25% compared to the growth expected by 2030. While digital transformations are changing the lives of people in smart cities, digital innovation is also steadily increasing. As shown in Fig. 7, there is steady raise in global gadget sales and applications [64, 65]. Suitable safety standards and security

**Fig. 7** Global Smart Gadget Market Sales



**Global Smart Gadget Market**
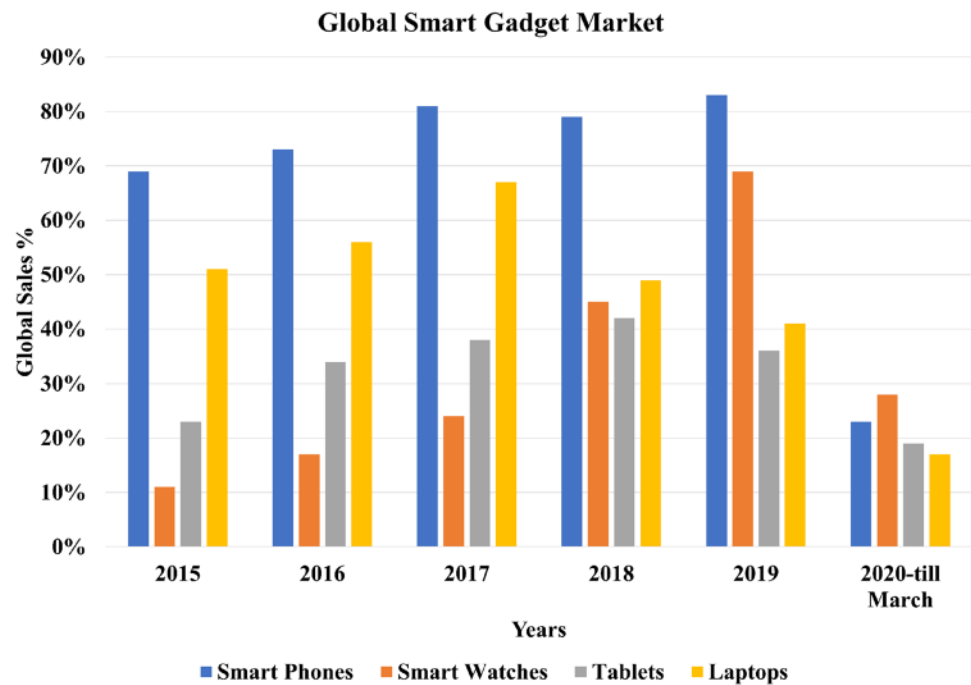
protocols are also required to protect digital devices as well as the user transactions. Thus, governments are allocating their resources in improving the security of these newly introduces digital technologies.

## NFC (Near Field Communication)

NFC enables the communication between two compatible devices over radio waves of specified frequencies. NFC-enabled devices can exchange without minimum power expenditure [66]. Many smartphones and smartwatches support NFC and leverage this technology to perform various everyday tasks, as shown in Fig. 8 [63]. NFC provides quick data transformation as the transmission frequency is 13.56 Megahertz.

## NFC for Healthcare Applications

Healthcare facilities should employ security mechanisms to protect both their physical resources (e.g., medical equipment and supplies) as well as the digital ones (e.g., user databases) from unauthorized users. NFC labels are used in medical clinics to screen supplies and assets. Staff and patient access control, and hardware global positioning frameworks (e.g., for the elderly) are other approaches that reinforce the safe operation of medical organizations [67]. Given the current COVID-19 pandemic, specialists encourage patients to remain at home and avoid visiting hospitals unless an emergency exists. Therefore, people with minor symptoms struggle to find treatment for their conditions. NFC-enabled medical devices and home medical services is

an interesting field that is receiving increasingly more attention especially in the unprecedented COVID-19 era [68–70].

NFC tags can be used to validate that patients are receiving genuine medicine and not counterfeit products. Furthermore, NFC tags can be employed to get useful medicine information just by scanning them with a smartphone. Such information include expiry date, potential symptoms, drug dosage, etc. The efficiency of NFC in reducing healthcare facility managing expenses, medicine counterfeiting is particularly useful for many applications. NFC-empowered gadgets are utilized in medical care and wellness applications both at home and in the healthcare clinics. Organizations are now embracing NFC to assist individuals monitor their health condition and symptoms.

## Contactless Payments with NFC

NFC can provide quick data transmission using 13.56 MHz as its main frequency. The three main components used during NFC payments include the cloud infrastructure, the client's devices (e.g., a smart phone), and the NFC reader, e.g., a point-of-sale (POS) device. Europay Mastercard Visa (EMV) is the standard used for NFC payments. NFC technology is a significant improvement over RFID, allowing users to transmit and collect data through over short ranges (roughly 10 cm). It works by connecting the reader and the payment devices over a wireless network. Apple pay, Google pay, and other digital electronic wallet payment applications utilize NFC payments, given that they are contactless, dynamically encrypted, and highly secure [71, 72]. When a

**Fig. 8** Overview of NFC-enabled devices and their applications
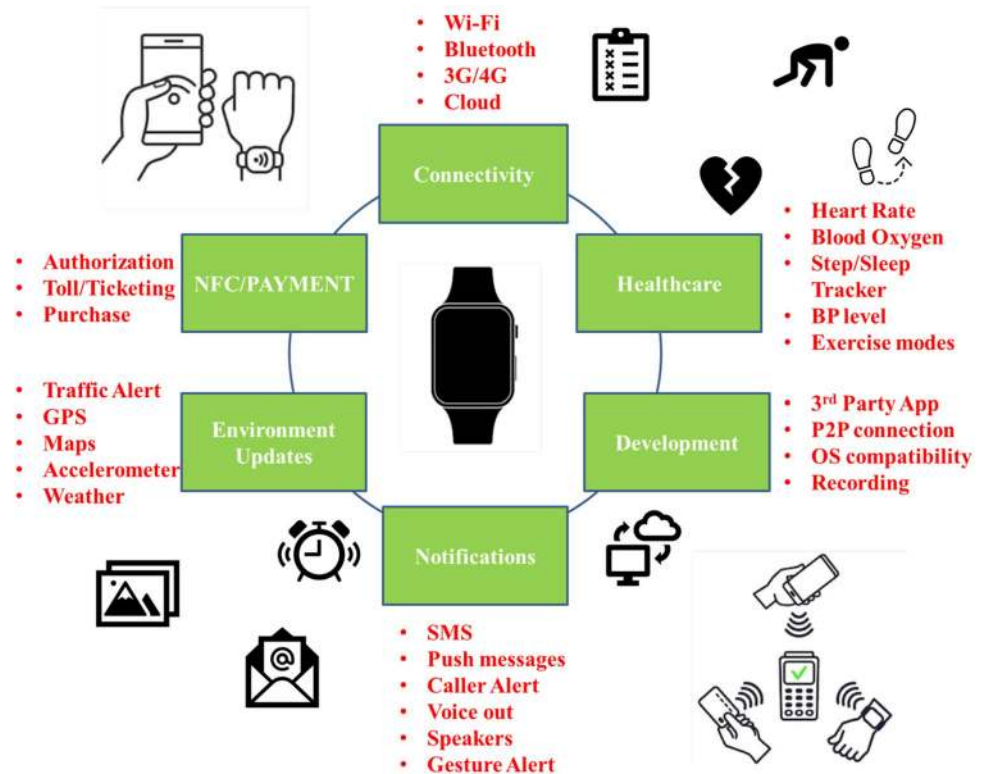


payment is initiated, the NFC controller inside smart mobile phones acts as a smart card and communicates with the NFC reader or POS device to exchange encrypted data enabling the transaction. Typical NFC-enabled devices can operate in three modes, i.e., the reader/writer mode, the peer-to-peer mode, and the card-emulation mode [73]:

1. *Reader/Writer mode* In the reader/writer mode, an NFC device behaves as a reader for NFC tags such as contactless smart cards and RFID tags. It detects a tag immediately and it can either read or write data to the tag which is detected.
2. *Peer-to-Peer mode* In the peer-to-peer mode, two NFC enabled devices can exchange information. This is the model used by Android Beam technology.
3. *Card-imitating mode*: In the card-imitating mode, an NFC device operates exactly like a contactless smart card. In this mode, the smartphone does not generate its own RF field; the NFC handles this process. However, the standard conventions encompassing ISO/IEC 14443 for traditional contactless cards have to be satisfied. In this mode, we can utilize our cell phone instead of credit/debit, travel cards, access or other types of cards,

etc. Thus, NFC-enabled devices allow users to perform transactions such as payments or ticketing.

NFC can streamline frictionless payments and is inherently more secure than RFID due to its frequency (13.56MHz), which requires the two chips—the shopper's and the retailer's—to be in close proximity to each other. In addition, NFC payments require the client (not the retailer as is the case with RFID) to initiate the transaction [52, 73, 74]. To guarantee security, NFC exchanges leverage single-use tokens and encrypted credentials. In such scenarios, an ephemeral one-time token is made for every transaction instead of requesting and communicating with the client's credit card system.

## Steps in NFC Payment

Cloud computing provides access to server resources and a database for NFC payments. It operates as a platform for storing customer credentials and transaction details. The operational sequence of NFC payments shown in Fig. 9, explains the series of steps followed during NFC payments and purchases. [4, 18, 75].

**Fig. 9** NFC Payment Steps
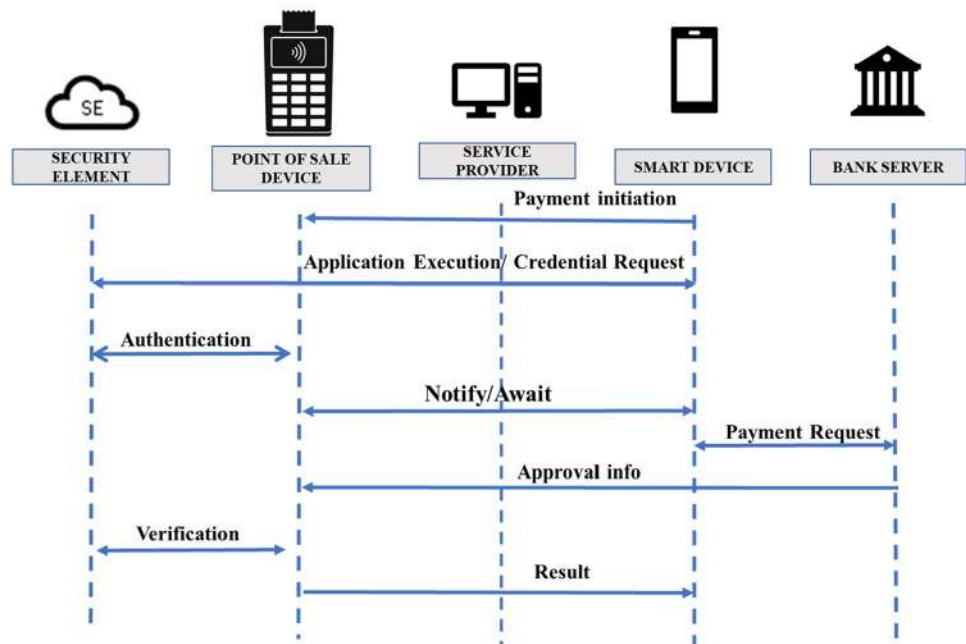


1. Purchase is initiated by scanning the NFC device over the POS device.
2. The POS device transmits a payment link from the cloud to the consumer device.
3. The POS requests credit limit validation, and payment authorization from the client's banking network.
4. Authorization granted to the POS from the cloud network.
5. Data validation and payment verification.
6. Merchant POS synchronizes with the client's record (if client transaction is approved).
7. Once approved, the mobile application is transferred to banking network for the payment.
8. The bank server verifies the credentials given by the user and processes the transaction.
9. The proof of the transaction is forwarded to the POS terminal by the bank server.
10. The POS device processes the payment and delivers the payment status receipt.

There are two main components in an NFC enabled smartphone: the security element (SE) and NFC controller. The SE is a processing unit that provides authentication for the requested transactions. NFC controllers act as the medium enabling the full duplex multi-cast handshake between the consumer NFC device and the POS terminal [73]. The SE is deployed as an algorithm operating on the cloud, whereas the NFC controller is embedded in the consumer devices and facilitates the storing of banking credentials and login details. Both NFC and SE must be synchronized before any application procedure initiation. Thus, consumer details are verified using SE (on the cloud resources), where it synchronizes with the banking network and establishes the communication gateway for payment processing. The transaction flow is as follows: (i) consumer NFC device-POS device communication, (ii) credential verification via SE and the bank network, (iii) payment initiation between NFC device and POS. Thus, both NFC and SE aid in the successful verification, authorization, and control of every step involved during consumer payment transactions.

## A Case Study of Utilizing BIC Technologies During COVID-19

In this case study, two types of analysis are performed in the five biggest smart cities in India for a period spanning from May 2019 to 2020 in different sectors such as agriculture, transportation, etc. This study demonstrates the inherent advantages that BIC technologies possess and how they can be leveraged to help smart cities handle the COVID-19 pandemic.

Algorithm 1 and the flowchart depicted in Fig. 10 detail

---

**Algorithm 1** Data Collection, Processing, Interpretation and Evaluation (COVID-19)

---

**function** SENSOR_DATA($Packet\_ID(Start)$)  ▷ —Obtained from Embedded IoT Devices

$Process \leftarrow Control\ Command\ [Init = Seq : Data]$  ▷ —Process Initiation

$Support_{Request} \leftarrow Software_{Packages+Patches}$  ▷ —Resource Check

$Select\ Tool + + \leftarrow Machine\ Learning :: Support\ Vectors$  ▷ —Machine Learning

Algorithm for Data Processing

$A_{route} \leftarrow \{Values\}$

$A_{Mode} \leftarrow \{Application\ Data\_Wireless :: NFC : Biometric\}$  ▷ —Data Resources

$Function_{Security} \leftarrow \{Data\ Signal\}$  ▷ —Security Analysis and Signal Test

$Start_{Derivative} \leftarrow \{Process :: Initiate\}$

$Time_{Arbitration} \leftarrow Sequence$

$Loop_{TimeCycle} \leftarrow Period$  ▷ —Signal strength check and Latency check

**for all** $Period \in \mathscr{R}_{Time,Date}$ **do**  ▷ —Period of Evaluation and Modelling

$\quad$ **for all** $\mathbf{P}' \in \mathscr{R}'_{Time,Date,Location} + Data$ **do**

$\quad\quad$ **if** $s(\mathbf{P}') = s(\mathbf{P}) + R'$ **then**

$\quad\quad\quad Data_R \leftarrow P_i(\mathbf{P}') - p_i(\mathbf{P})$

$\quad\quad\quad Train_c \leftarrow P_j(\mathbf{P}') - p_j(\mathbf{P})$

$\quad\quad\quad Data \leftarrow \{[Train_R]^+ [Add_R]^- [Data_R]^+ [Train+Validate]^{Function}\}$  ▷ —Data Check and verification

$\quad\quad\quad initiate_{Security\ check} \leftarrow [Protocol](start(\mathbf{P})/Level) - Check(P(\mathbf{P}'))$

$\quad\quad\quad Start_{Process} \leftarrow P_{Map} + +$

$\quad\quad\quad$ **if** $P_{Training} = Validation\mathrm{Map} - Check\_P'$ **then**

$\quad\quad\quad\quad P'_{Process} \leftarrow \{Data :: R\}$

$\quad\quad\quad$ **else if** $Initiate_{Interpretation} == \mathrm{Guideline} - Value$ **then**

$\quad\quad\quad\quad Check_{Data\ set} \leftarrow \{Data\ Pack\ Size\}$

$\quad\quad\quad$ **else if** $Train_R = Machine\_learning\_\mathrm{Check} - [response]$ **then**

$\quad\quad\quad\quad P_{Analysis} \leftarrow \{R, P, P'\}$

$\quad\quad\quad$ **end if**

$\quad\quad\quad$ **if** $Data\ set == Not\ Sufficient :: Req\_Resource$ **then** ▷ —Data acquired from Client through various IoT enabled Resources

$\quad\quad\quad\quad Check_{Signal} \leftarrow Initiate_{IoT\ device} + +$

$\quad\quad\quad\quad Test\_Data \leftarrow Plot_{P+R::P'} + Validate_{Plot}$

$\quad\quad\quad\quad$ **if** $Validate(P + +(\mathbf{P}'), R) == Fail$ **then**

$\quad\quad\quad\quad\quad Process_{Re-check} \leftarrow Data_{P::P'} + Function$

$\quad\quad\quad\quad$ **end if**

$\quad\quad\quad$ **else if** $Package(P :: (\mathbf{P}'), [Software]) == Request + +$ **then**  ▷ —Software Patch Update

$\quad\quad\quad\quad Train\_data \leftarrow Function_R + Test\_Data$

$\quad\quad\quad\quad Validation_{Check} \leftarrow [Credential_{Authenticity} + Protocol]$  ▷ —Authentication and Validation of Data

**Fig. 10** Flowchart for data processing and interpretation using machine learning algorithms
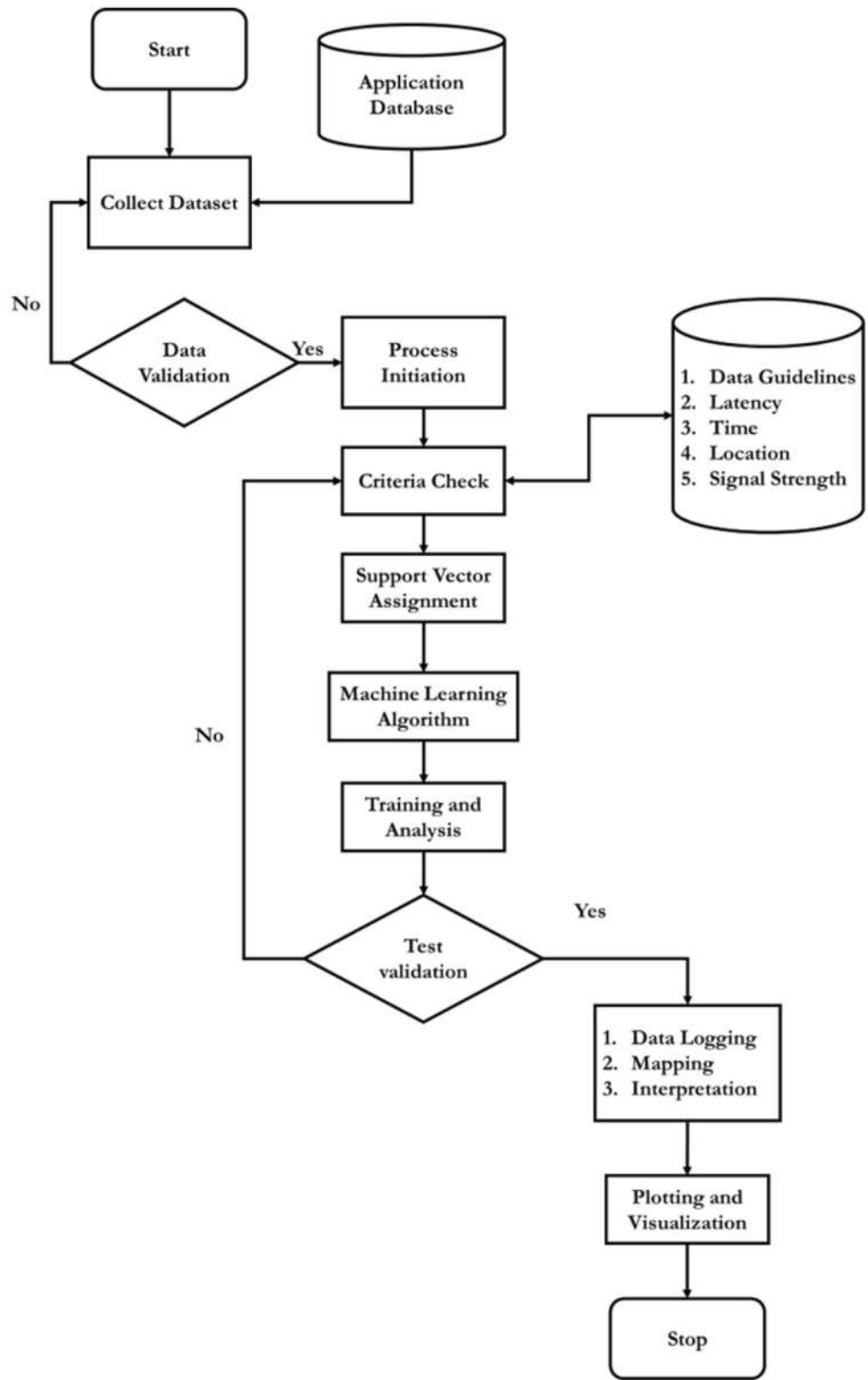


the processes involved in gathering, processing, and analyzing data from BIC resources. The flowchart shows the operation sequences and illustrates the steps starting from data collection to interpretation and validation. In each step of the operation, the source of data is validated using the guidelines and rules from different operating agencies. During the validation steps if data are violated or mismatched, the process is re-initiated. The test interpretation and validation are made visually available to the authorized government agencies [65, 76]. The algorithm can be customized in real-time depending on the application and use case. Data packets are obtained from embedded IoT devices and loaded with
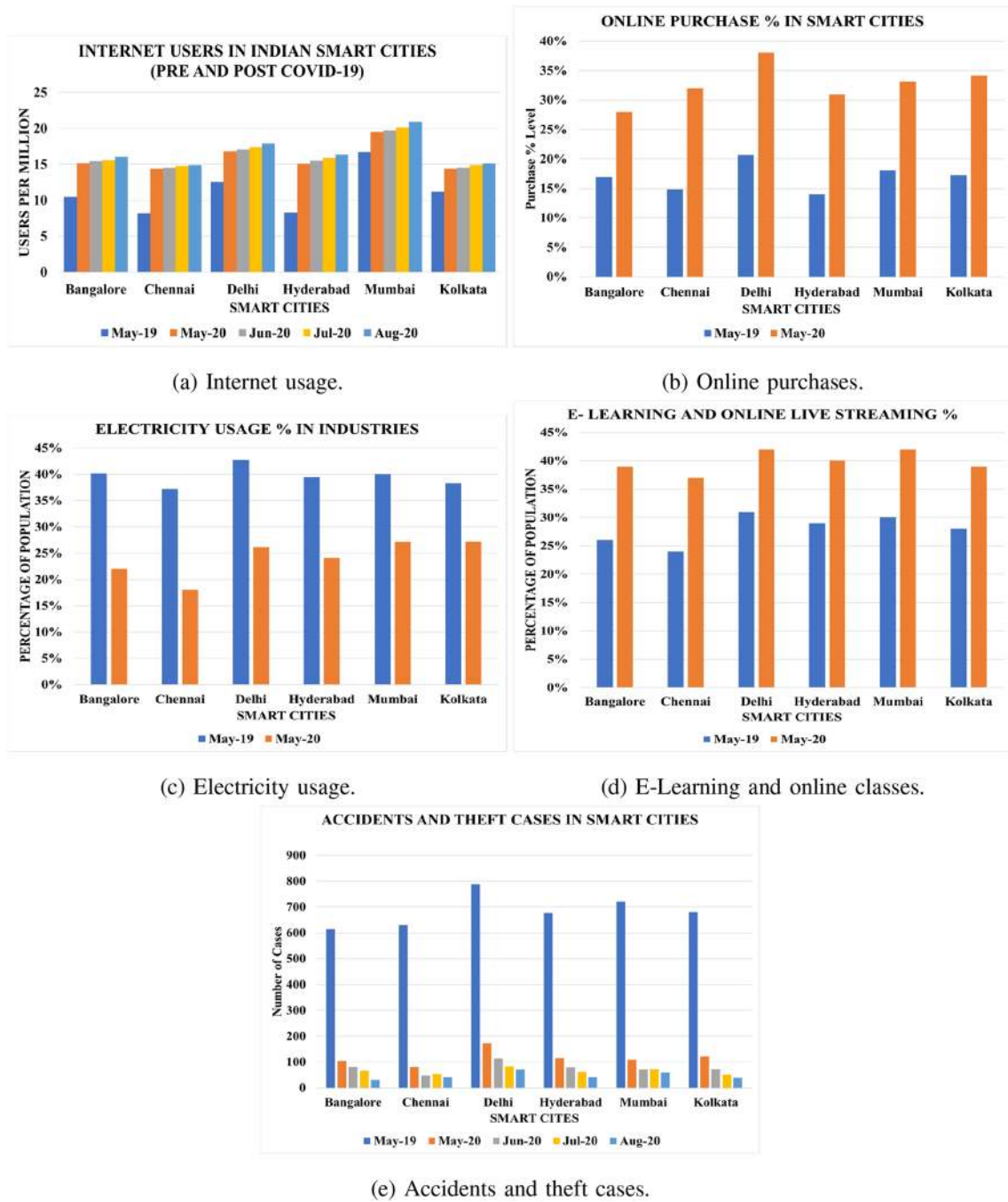
(a) Internet usage.



(b) Online purchases.



(c) Electricity usage.



(d) E-Learning and online classes.



(e) Accidents and theft cases.

**Fig. 11** Case studies on the impact of COVID-19 in different cities within India

suitable control and execution sequences. Both parametric (numerical data) and non-parametric (weights and percentages) data sets can be loaded and modelled. During the process initiation, modelling tools and machine learning algorithms along with evaluation criteria need to be predefined. The data iterations are segmented based on time, usage, latency, and collection intervals. The data can vary with time and location, thus suitable correlation and evaluation is done before modelling the data providing useful insights. The

process is initiated once the valid data sets are obtained for the modelling and training steps. During the training and analysis stages, the error values will be eliminated to obtain the best fit that will satisfy the predefined criteria. The credibility and validity of data are verified at regular time intervals as shown in Algorithm 1. Once the training, testing, and modelling are completed, the mapping and interpretation are done based on the data set source, application and functions.

**Table 1** Impact of COVID-19 in different sectors of Indian cities: a case study using CT-BIC

| Sector | Bangalore (%) | Chennai (%) | Delhi (%) | Hyderabad (%) | Mumbai (%) | Kolkata (%) |
|---|---|---|---|---|---|---|
| Financial Service | − 16.3 | − 12.4 | − 14.71 | − 13.8 | − 16.8 | − 10.21 |
| Real Estate | − 14.5 | − 13.3 | − 14.43 | − 12.11 | − 17.43 | − 10.3 |
| Mining and Quarry | − 7.8 | − 6.17 | − 7.3 | − 4.10 | − 5.41 | − 3.98 |
| Manufacturing | − 8.5 | − 5.53 | − 9.32 | − 4.40 | − 7.11 | − 6.61 |
| Agriculture | − 6.1 | − 7.3 | − 5.51 | − 4.38 | − 5.32 | − 4.81 |
| Fishing and Forestry | − 5.3 | − 4.23 | − 3.17 | − 3.82 | − 4.20 | − 3.4 |
| Broadcasting | − 9.3 | − 7.7 | − 8.03 | − 7.20 | − 7.89 | − 8.81 |
| Transportation | − 10.6 | − 9.12 | − 11.15 | − 9.10 | − 16.81 | − 13.21 |
| Defence and Public Work | − 1.3 | − 1.28 | − 1.81 | − 1.39 | − 2.21 | − 2.08 |
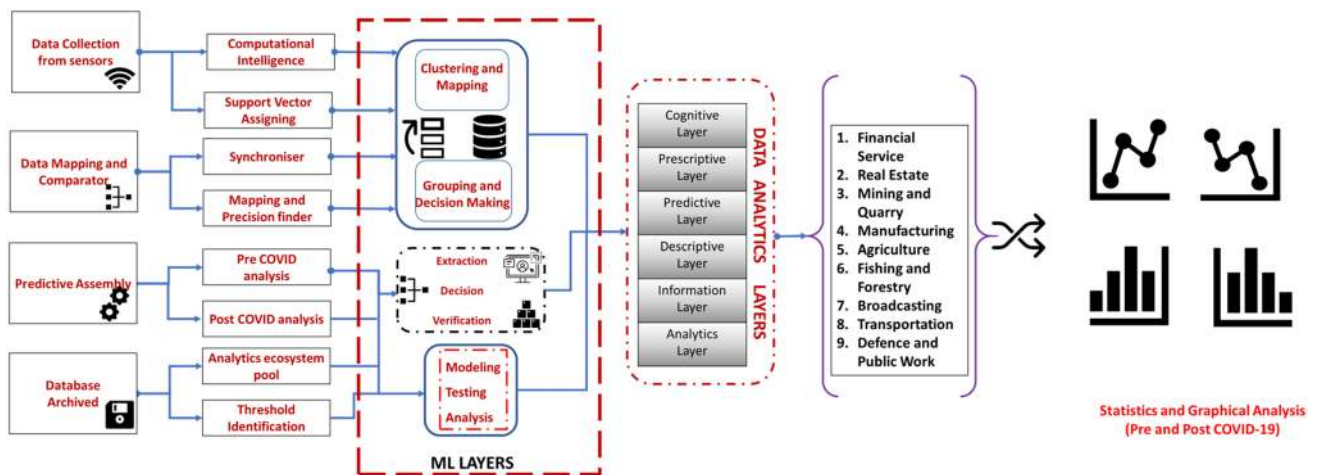


**Fig. 12** Machine learning and data analytics model: case study on different sectors in smart cities

Survey results are presented to showcase the impact of COVID-19 and the effective usage of BIC in various sectors of smart cities. Data generated from different embedded devices are recorded periodically and updates are made at the government authorized data centers [10, 11, 77–79]. According to the statistical survey results and data obtained from government agencies, cities that are ICT-integrated are performing better compared to the other less digitized cities in India [63, 64, 76]. As shown in Fig. 11, the data obtained from various smart cities demonstrate better overall performance in May 2019 than May 2020 due to COVID-19. The data are collected over period of 1 year and investigate different parameters like internet usage, Fig. (11a), online purchase (Fig. 11b), electricity consumption (Fig. 11c), and e-learning (Fig. 11d) [33]. Some of the studies include data from state websites such as accidents and theft analyses as shown in Fig. 11e. Data generated from embedded devices are connected from local (closed-circuit television) CCTV cameras, digital electricity meters, internet service providers, and local municipal web servers. Then, data analytics and machine learning algorithms are applied to the aggregated data. In this study, *K*-means clustering ML is used to evaluate the actual raw data from sensors and compare them with data available from government websites. Since curfew and nationwide lockdown were employed from March 2020 and got extended with few relaxations, COVID-19 drastically affected many industries [80] .

Since the cases of COVID-19 are/were increasing, keeping records from the health sector is critical. Furthermore, since data are recorded at all possible access points, manual observation and extraction is not required. Furthermore, the pool of data-collecting sensors available on the embedded devices must be handled efficiently. The prime idea behind implementing IoT based data collecting modules, big data-based classification, and cloud-based remote assistance is to monitor the operational status of these modules without time delays and with resource anonymity. The command line executions from different operating sensors are secured using authorization codes and access control protocols before their commands are being executed in real-time. In such deployments, network gateways are utilized to enhance security. Consider the BIC model, as shown in Fig. 12, where the

data are processed inside the manufacturing unit [81]. The model shows the detailed processes involved during the design, collection, processing and analysis of data collected from various sectors in India and help understand the impact of COVID-19. Predictive data analytics and machine learning models are used to interpret and map the data of different affected sectors in India. Various government agencies are actively involved in updating the data using their ICT infrastructure. Many central statistical data collection agencies are being involved to project the impact of COVID-19 [63, 64]. The databases are cumulatively modelled enhancing the understanding of the pandemic impacts on a global level. This investigation can help understand how different sectors are impacted by COVID-19, as shown in Table 1 [82–85]. The COVID-19 outbreak caused negative impacts on the country's economic growth irrespective of the sector, according to statistical analyses performed from various government agencies [64, 76, 86, 87]. It is also estimated that the recovery time for cities to perform and compete in the global market is also drastically affected.

During the entire analysis process (pre and post COVID-19), both actual and existing data were obtained and a lot of computational analysis, ML algorithms, and data analytics were done for feature extraction, modelling, and evaluation. For the initial segregation and analysis, clustered data were considered. Support vector machine learning (SVML) was used for the vector classification of the obtained data. These vectors were assigned after applying and clustering the data using K-mean clustering. The scaling factor obtained using cluster formations, and vector classification— used for the prediction and analysis of different components after a series of data analytic procedures—is called smart safe factor (SSF). Consider the sample on which the SSF model

applied for predicting the number of industries affected between March 2020 and June 2020. The data is clustered on a regular basis and it is given as the input for analyzing the actual versus the available ratio for that particular sector and day. The SSF obtained will be used to find the predictive model of actual versus existing per day in the industry sector without leaving stocks on-hold over an extended time period and while running successfully in this pandemic situation. After getting the data of the sector, cluster partition is done using K-mean clustering ML. In this technique, the data for each sector will be given as input for vector combinations. From the clustering and mapping, data about the stocks, usage, and assembly different components were obtained. The following results were obtained using K-mean clustering ML for any automobile industry:

1. Pre COVID-19state versus post COVID-19 data.
2. Market stocks.
3. Resources (before and after COVID-19).
4. Profit-loss ratio.
5. Production.
6. Sales and clearance levels.
7. Stock-in and stock-out ratios.
8. Waste and scrap per day.

With SVML, clustered data are assigned to vectors, and linearization is done on those data during pre- and post-processing. With SSF, the extracted data are modeled, tested, and given as input for the analytics layer, where using the SSF predictions, the data will be columnized and identified with the desired vectors and cluster-IDs. Thus, vectors and clusters along with SSF tend to predict the margin of all the data required for a complete case study in each sector. In



**Fig. 13** Impact of COVID-19 on the pollution level of smart cities
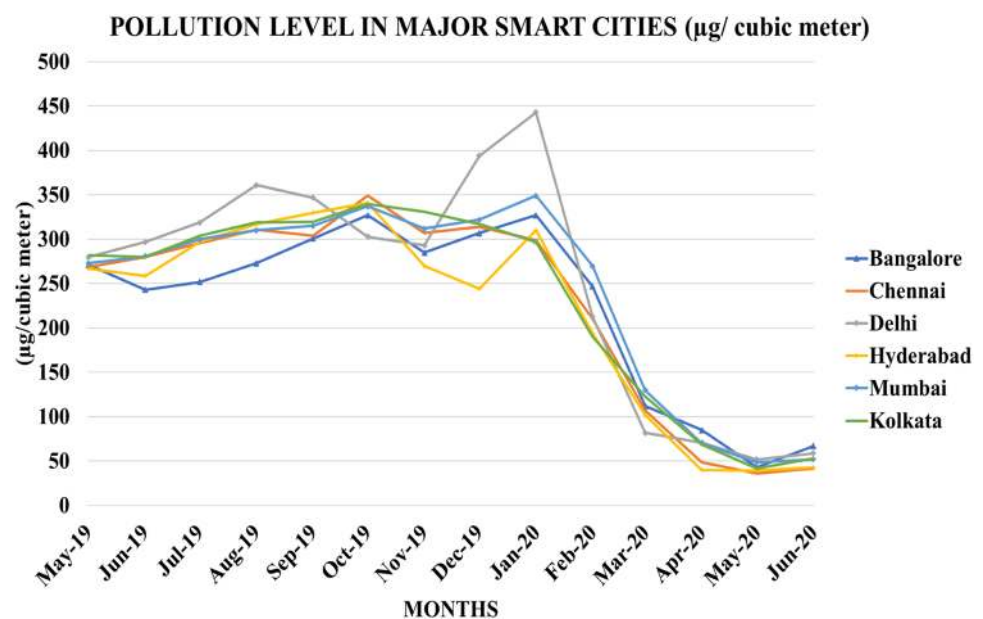
this case study, different sectors are considered from different smart cities in India. An example derived from and automobile manufacturing sector case study is demonstrated in Fig. 12.

Vehicle design and assembly units are investigated to improve and make the workplace a completely automated and energy efficient system. With the detailed analysis and survey of the existing workplace environments, the industrial units are analyzed for obsolete functions and abnormalities. A field study by expert research communities was conducted for data collection, visualization, and critical area identification. Following this case study approach, we have adapted the dynamic nationwide lockdown rules, preliminary modelling tools, and developed a machine learning model [65, 76, 86, 87].

This developed model is programmed using linear regression single line restructuring entities and encoded in the R coding platform. Classification, segmentation, and analysis includes results from market stocks, process control management schemes, day/monthly business analytics, and structural mapping of different components during the final product delivery. Data sets and results from the developed model help forecast the automaker industry and boost its production in all aspects from assembly to commercialization on a long-term basis. The result is graphically studied and SSF is statistically evaluated using linear regression models and statistical data analytic methods. Final data forecasting is obtained from the regression model analysis and used for restructuring of actual data over the period from May 2019 to 2020. The complete package is installed in respective industries to mitigate all types of losses and it is used as a restructuring formulation tool for long-term load and cost forecasting in the stock vending, production, polishing, and assembly sections. In this study, we also tried to analyze the pollution levels shown in Fig. 13, in different smart cities in India and check the impact of COVID-19 [84, 88, 89]. This can help the government as well as various industries to forecast, withstand, and survive the pandemic. Collection, plotting, and analysis of pollution data in smart cities illustrates the typical usage of ICT and can help improve the environmental conditions. Furthermore, pollution due to industrial waste (both processed and unprocessed) must be controlled and mandatory pollution level testing could be required to address these issues [63, 87] .

## Discussion on the Implications of Utilizing BIC

Focusing on smart cities, both before and after COVID-19, BIC as well as CT greatly assisted in managing the consumer needs and the data collection during the pandemic crisis. The following denote the implications of using BIC in smart cities.

## Practical Implications

This study has significant implications in understanding the BIC applications and its effectiveness in smart cities. In this study, a detailed overview of the CT available for smart cities where explained. We have studied the BIC with respect to different sectors in Indian smart cities and our detailed survey shows the effect of BIC in data collection, processing and results for identifying the worst affected sectors in each of the smart cities of India. The model is developed to showcase the data processing and other functions that are obtained from the embedded devices. In this study, the impact of COVID-19 is also taken into account to validate the effectiveness of BIC in smart cities. Furthermore, a better understanding of data models, sequence generation algorithms, and steps involved with different BIC techniques and applications are explained. Since the entire BIC completely relies on data that are generated from embedded devices, sensors, and components, computational resources are required to process those data.

## Limitations of Study

Data obtained from official government websites and state-wise portals are reliable for training machine learning models but while analyzing the data using model predictors, the vectors do not match with the models that are obtained when training using SVML and clustering analysis. Steep rise or sudden fall in 1 day of COVID-19 data had big impacts on determining the actual status prevailing in those states. This condition is mainly due to the inactive updating of the sector information made by the department officials. Predictive modelling and cluster formation require eigenvectors and Bayesian filter values which are obtained only after training the entire data set within the predefined time period. Short-span calculations, complex operations, and insufficient inhibit the prediction accuracy of such models.

Anonymity is available from the data provided by each regulating authority. However, the severity of COVID-19 led these smart cities to lockdowns inflicting resource restrictions during data collection, processing, and analysis. Upon evaluating the data with suitable ML models, results do not correlate due to the lack of validation factors and seasonal interference impacting the effectiveness of the developed model. The heuristic data impact the prediction accuracy of the vector and filter functions as well as the forecasting of the impacts on smart cities due to COVID-19. Furthermore, data from the healthcare sector are not easily obtained due to the potential unwanted consequences that negative

predictions can have on the public. Thus, government agencies are strictly monitoring such data, allowing responsible and restricted disclosure.

# Conclusion

Science and technology have become the key drivers of rapid urbanization and introduction of the smart city concept. The uncertainty caused by the COVID-19 pandemic paved the way for the development of CT globally. In this paper, we present a comprehensive survey of CT applications in smart cities using BIC technologies. Following, we discuss case studies from five smart cities in India which are using CT and BIC in many applications. We offer a detailed analysis on the different sectors within smart cities that the COVID-19 impacts mandated the use of BIC. We compile the survey results and provide insights on CT applications in various smart cities and how they certain sectors were affected by COVID-19. In our future work, we plan to investigate the challenges of implementing CT in highly populated countries, like India, and demonstrate the effectiveness of BIC in areas such as data collection, processing, and analysis to address current issues and open problems existing in smart city infrastructures.

## Declarations

**Conflicts of Interest** On behalf of all authors, the corresponding author states that there is no conflict of interest.

# References

1. Nations U. World urbanization prospects: the 2018 revision, key facts. Technical report, 2018.
2. Djahel S, Doolan R, Muntean G-M, Murphy J. A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches. IEEE Commun Surveys Tutor. 2014;17(1):125–51.
3. Kaur MJ, Maheshwari P. Building smart cities applications using IoT and cloud-based architectures. In: 2016 International Conference on industrial informatics and computer systems (CIICS), IEEE, 2016, p. 1–5.
4. Jiang D, Zhang P, Lv Z, Song H. Energy-efficient multi-constraint routing algorithm with load balancing for smart city applications. IEEE Internet of Things J. 2016;3(6):1437–47.
5. Sayghe A, Hu Y, Zografopoulos I, Liu X, Dutta RG, Jin, Y, Konstantinou C. Survey of machine learning methods for detecting false data injection attacks in power systems. IET Smart Grid. 2020;3:581–595. https://doi.org/10.1049/iet-stg.2020.0015.
6. Lam AY, Leung Y-W, Chu X. Electric vehicle charging station placement: formulation, complexity, and solutions. IEEE Trans Smart Grid. 2014;5(6):2846–56.
7. Naphade M, Banavar G, Harrison C, Paraszczak J, Morris R. Smarter cities and their innovation challenges. Computer. 2011;44(6):32–9.
8. Lee J, Guo J, Choi JK, Zukerman M. Distributed energy trading in microgrids: a game-theoretic model and its equilibrium analysis. IEEE Trans Ind Electron. 2015;62(6):3524–33.
9. Manimuthu A, Ramesh R. Privacy and data security for grid-connected home area network using internet of things. IET Netw. 2018;7(6):445–52.
10. Aidasani LK, Bhadkamkar H, Kashyap AK. Iot: the kernel of smart cities. In: 2017 Third International Conference on science technology engineering & management (ICONSTEM). IEEE, 2017, p. 8–11.
11. Arasteh H, Hosseinnezhad V, Loia V, Tommasetti A, Troisi O, Shafie-khah M, Siano P. Iot-based smart cities: a survey. In: 2016 IEEE 16th International Conference on environment and electrical engineering (EEEIC). IEEE, 2016, p. 1–6.
12. Aráuz J. Smart cities and the dire need for a course correction. In: IEEE International Smart Cities Conference (ISC2). IEEE. 2018;2018; p. 1–6.
13. Baccarelli E, Naranjo PGV, Scarpiniti M, Shojafar M, Abawajy JH. Fog of everything: Energy-efficient networked computing architectures, research challenges, and a case study. IEEE Access. 2017;5:9882–910.
14. Colistra J. The evolving architecture of smart cities. In: IEEE International Smart Cities Conference (ISC2). IEEE. 2018;2018; p. 1–8.
15. Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: challenges and opportunities. IEEE Access. 2018;6:46 134-46 135.
16. Konstantinou C. Towards a secure and resilient all-renewable energy grid for smart cities. In: IEEE Consumer Electronics Magazine, pp. 1–1, 2021.
17. He H. Research on the application of electronic technology of internet of things in smart city. In: 2020 International Conference on intelligent transportation, big data & smart city (ICITBS). IEEE, 2020, p. 454–57.
18. Jabbar M, Aluvalu R. Smart cities in India: Are we smart enough? In: International Conference on smart technologies for smart nation (SmartTechCon). IEEE. 2017;2017, p. 1023–26.
19. Jalali R, El-Khatib K, McGregor C. Smart city architecture for community level services through the internet of things. In: 2015 18th International Conference on intelligence in next generation networks. IEEE, 2015, p. 108–113.
20. Manimuthu A, Dharshini V. Framework for load power consumption in Han using machine learning and IoT assistance. IEEE Design Test, pp. 1–1, 2020.
21. Minoli D, Sohraby K, Occhiogrosso B. Iot considerations, requirements, and architectures for smart buildings-energy optimization and next-generation building management systems. IEEE Internet of Things J. 2017;4(1):269–83.
22. Perera C, Liu CH, Jayawardena S. The emerging internet of things marketplace from an industrial perspective: a survey. IEEE Trans Emerg To Comput. 2015;3(4):585–98.
23. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. IEEE Internet of Things J. 2014;1(1):22–32.
24. Xenofontos C, Zografopoulos I, Konstantinou C, Jolfaei A, Khan MK, Choo KKR. Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies. In: IEEE Internet of Things J. 2021; p. 1.

25. Jin J, Gubbi J, Marusic S, Palaniswami M. An information framework for creating a smart city through internet of things. IEEE Internet of Things J. 2014;1(2):112–21.

26. Zografopoulos I, Ospina J, Liu X, Konstantinou C. Cyber-physical energy systems security: threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access. 2021;9:29 775-29 818.

27. Kuruvila AP, Zografopoulos I, Basu K, Konstantinou C. Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids. International Journal of Electrical Power & Energy Systems. 2021;132:107150.

28. Kiliç T, Tuncer T. Smart city application: Android based smart parking system. In: International Artificial Intelligence and Data Processing Symposium (IDAP). IEEE. 2017;2017, p. 1–4.

29. Kirimtat A, Krejcar O, Kertesz A, Tasgetiren MF. Future trends and current state of smart city concepts: a survey. IEEE Access. 2020;8:86 448-86 467.

30. Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Commu Surveys Tutor. 2014;16(4):1933–54.

31. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J. 2017;4(5):1125–42.

32. Li Y, Dai W, Ming Z, Qiu M. Privacy protection for preventing data over-collection in smart city. IEEE Trans Comput. 2015;65(5):1339–50.

33. Manimuthu A, Ramadoss R. Absolute energy routing and real-time power monitoring for grid-connected distribution networks. IEEE Design Test. 2019;36(2):88–96.

34. Moreno MV, Terroso-Sáenz F, González-Vidal A, Valdés-Vela M, Skarmeta AF, Zamora MA, Chang V. Applicability of big data techniques to smart cities deployments. IEEE Trans Ind Inf. 2016;13(2):800–9.

35. Mulero R, Almeida A, Azkune G, Abril-Jiménez P, Waldmeyer MTA, Castrillo MP, Patrono L, Rametta P, Sergi I. An iot-aware approach for elderly-friendly cities. IEEE Access. 2018;6:7941–57.

36. Pai P, Shashikala K. Smart city services-challenges and approach. In: 2019 International Conference on machine learning, big data, cloud and parallel computing (COMITCon). IEEE, 2019, p. 553–58.

37. Vatsa M, Nixon MS. Editorial introducing the IEEE transactions on biometrics, behavior, and identity science. IEEE Trans Biomet Behav Identity Sci. 2019;1(1):1–2.

38. Pradhan MA, Patankar S, Shinde A, Shivarkar V, Phadatare P. Iot for smart city: Improvising smart environment. In: 2017 International Conference on energy, communication, data analytics and soft computing (ICECDS). IEEE, 2017, p. 2003–2006.

39. Sookhak M, Tang H, He Y, Yu FR. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun Surveys Tutor. 2018;21(2):1718–43.

40. Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: vision and challenges. IEEE Internet of Things J. 2016;3(5):637–46.

41. Sun Y, Song H, Jara AJ, Bie R. Internet of things and big data analytics for smart and connected communities. IEEE Access. 2016;4:766–73.

42. Dhawan AP, Heetderks WJ, Pavel M, Acharya S, Akay M, Mairal A, Wheeler B, Dacso CC, Sunder T, Lovell N, Gerber M, Shah M, Senthilvel SG, Wang MD, Bhargava B. Current and future challenges in point-of-care technologies: a paradigm-shift in affordable global healthcare with personalized and preventive medicine. IEEE J Transl Eng Health Med. 2015;3:1–10.

43. Yao H, Wang C, Fu X, Liu C, Wu B, Li F. A privacy-preserving rlwe-based remote biometric authentication scheme for single and multi-server environments. IEEE Access. 2019;7:109 597-109 611.

44. Zhou K, Ren J. Passbio: privacy-preserving user-centric biometric authentication. IEEE Trans Inf For Secur. 2018;13(12):3050–63.

45. Liu C, Hu X, Zhang Q, Wei J, Liu W. An efficient biometric identification in cloud computing with enhanced privacy security. IEEE Access. 2019;7:105 363-105 375.

46. Kwon T, Moon H. Biometric authentication for border control applications. IEEE Trans Knowl Data Eng. 2008;20(8):1091–6.

47. Gonzalez-Sosa E, Vera-Rodriguez R, Fierrez J, Patel VM. Exploring body shape from mmw images for person recognition. IEEE Trans Inf For Secur. 2017;12(9):2078–89.

48. Poh N, Bourlai T, Kittler J, Allano L, Alonso-Fernandez F, Ambekar O, Baker J, Dorizzi B, Fatukasi O, Fierrez J, Ganster H, Ortega-Garcia J, Maurer D, Salah AA, Scheidat T, Vielhauer C. Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms. IEEE Trans Inf For Secur. 2009;4(4):849–66.

49. Robertson JJ, Guest RM, Elliott SJ, O'Connor K. A framework for biometric and interaction performance assessment of automated border control processes. IEEE Trans Hum-Mach Syst. 2017;47(6):983–93.

50. Kamgar-Parsi B, Lawson W, Kamgar-Parsi B. Toward development of a face recognition system for watchlist surveillance. IEEE Trans Pattern Anal Mach Intell. 2011;33(10):1925–37.

51. Xu H, Veldhuis RNJ, Kevenaar TAM, Akkermans TAHM. A fast minutiae-based fingerprint recognition system. IEEE Syst J. 2009;3(4):418–27.

52. Ortega-Delcampo D, Conde C, Palacios-Alonso D, Cabello E. Border control morphing attack detection with a convolutional neural network de-morphing approach. IEEE Access. 2020;8:92 301-92 313.

53. Kuutti S, Fallah S, Katsaros K, Dianati M, Mccullough F, Mouzakitis A. A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications. IEEE Internet of Things J. 2018;5(2):829–46.

54. Minovski D, Åhlund C, Mitra K. Modeling quality of iot experience in autonomous vehicles. IEEE Internet of Things J. 2020;7(5):3833–49.

55. Gao Y, Ai Y, Tian B, Chen L, Wang J, Cao D, Wang F. Parallel end-to-end autonomous mining: an iot-oriented approach. IEEE Internet of Things J. 2020;7(2):1011–23.

56. Solorio JA, Garcia-Bravo JM, Newell BA. Voice activated semi-autonomous vehicle using off the shelf home automation hardware. IEEE Internet of Things J. 2018;5(6):5046–54.

57. Gao K, Wang B, Xiao L, Mei G. Incomplete road information imputation using parallel interpolation to enhance the safety of autonomous driving. IEEE Access. 2020;8:25 420-25 430.

58. Sadhukhan P. An iot based framework for smart city services. In: 2018 International Conference on communication, computing and internet of things (IC3IoT). IEEE, 2018, p. 376–79.

59. Vakula D, Kolli YK. Low cost smart parking system for smart cities. In: 2017 International Conference on intelligent sustainable systems (ICISS). IEEE, 2017, p. 280–284.

60. Wieclaw L, Pasichnyk V, Kunanets N, Duda O, Matsiuk O, Falat P. Cloud computing technologies in "smart city" projects. In: 2017 9th IEEE International Conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), vol. 1. IEEE, 2017, p. 339–42.

61. Zhang Q, Yang LT, Chen Z. Privacy preserving deep computation model on cloud for big data feature learning. IEEE Trans Comput. 2015;65(5):1351–62.

62. Babin BJ, Zikmund WG. Exploring marketing research. Cengage Learning. 2015.

63. Liu S. Smart cities—statistics & facts. 2020. https://www.statista.com/topics/4448/smart-city/#dossierSummary Accessed 25 May 2020.

64. "Smart city index," https://www.imd.org/smart-city-observatory/Home/, 2019. Accessed 6 Nov 2020.

65. "Housing and urban affairs," http://mohua.gov.in/, 2019–2020. Accessed 17 Oct 2020.

66. Tavakoli A, Faghihinia A, Kalhor A. An innovative test bed for verification of attitude control system. IEEE Aerosp Electron Syst Mag. 2017;32(6):16–22.

67. Sethia D, Gupta D, Mittal T, Arora U, Saran H. Nfc based secure mobile healthcare system. In: Sixth International Conference on communication systems and networks (COMSNETS). 2014;2014, p. 1–6.

68. Ukalkar GV, Halgaonkar PS. Cloud based nfc health card system. In: International Conference on intelligent computing and control systems (ICICCS). 2017;2017, p. 436–41.

69. Jara AJ, Lopez P, Fernandez D, Zamora MA, Ubeda B, Skarmeta AF. Communication protocol for enabling continuous monitoring of elderly people through near field communications. Interact Comput. 2014;26(2):145–68.

70. Jiang Y, Pan K, Leng T, Hu Z. Smart textile integrated wireless powered near field communication body temperature and sweat sensing system. IEEE J Electromagn RF Microw Med Biol. 2020;4(3):164–70.

71. Phang S, Ivrlač MT, Gradoni G, Creagh SC, Tanner G, Nossek JA. Near-field mimo communication links. IEEE Trans Circ Syst I Regul Papers. 2018;65(9):3027–36.

72. Jin R, Du X, Deng Z, Zeng K, Xu J. Practical secret key agreement for full-duplex near field communications. IEEE Trans Mob Comput. 2016;15(4):938–51.

73. Garnica J, Chinga RA, Lin J. Wireless power transmission: from far field to near field. Proc IEEE. 2013;101(6):1321–31.

74. Tak Y, Nam S. Extended mode-based bandwidth analysis for asymmetric near-field communication systems. IEEE Trans Antennas Propag. 2012;60(1):421–4.

75. Sharifi A, Khavarian-Garmsir AR. The covid-19 pandemic: Impacts on cities and major lessons for urban planning, design, and management. Sci Total Environ. 2020;749: p. 142391.

76. "Data," https://data.gov.in/, 2019-2020. Accessed 22 Oct 2020.

77. Fusilier M, Durlabhji S. An exploration of student internet use in India: the technology acceptance model and the theory of planned behaviour. Campus-Wide Information Systems. 2005 Sep 1.

78. Rajhans V, Memon U, Patil V, Goyal A. Impact of covid-19 on academic activities and way forward in Indian optometry. J Optomet. 2020;13(4):216–26.

79. Kumar M, Dwivedi S. Impact of coronavirus imposed lockdown on Indian population and their habits. Int J Sci Healthc Res. 2020;5(2):88–97.

80. Ospina J, Liu X, Konstantinou C, Dvorkin Y. On the feasibility of load-changing attacks in power systems during the covid-19 pandemic. IEEE Access. 2021;9:2545–63.

81. Lokhandwala S, Gautam P. Indirect impact of covid-19 on environment: A brief study in Indian context. Environ Res. 2020;188:109807.

82. Dong H, Yang F, Lu X, Hao W. Internet addiction and related psychological factors among children and adolescents in china during the coronavirus disease 2019 (covid-19) epidemic. Front Psychiatry. 2020;11:751.

83. Pandey N, Pal A, et al. Impact of digital surge during covid-19 pandemic: a viewpoint on research and practice. Int J Inf Manag. 2020;55:102171.

84. Singh RP, Chauhan A. Impact of lockdown on air quality in India during covid-19 pandemic. Air Qual Atmos Health. 2020;13(8):921–8.

85. Rajendran S, Pagel E. Insights on next-generation manufacturing of smart devices using text analytics. Heliyon. 2020;6(7):e04491.

86. "Housing technology," https://ghtc-india.gov.in/, 2019-2020. Accessed 3 Nov 2020.

87. "Digital india," https://www.digitalindia.gov.in/, 2019-2020. Accessed 8 Oct 2020.

88. Mele M, Magazzino C. Pollution, economic growth, and covid-19 deaths in India: a machine learning evidence. Environ Sci Pollut Res. 2021;28(3):2669–77.

89. Mahato S, Pal S, Ghosh KG. Effect of lockdown amid covid-19 pandemic on air quality of the megacity Delhi, India. Sci Total Environ. 2020;730:139086.