SECURITY CHALLENGES IN SMART CITIES

KAUSTHUB KODAMAGULLA
SHRUTHI REDDY KAMIDI
NAGASAI THADISHETTY

Agenda

- What/Why is Smart City?
- How Smart City Works?
- History and State Of Art
- Challenges in the Smart City
- Solutions
- Technologies involved
- Our insights on the topic
- Conclusion

WHO CAME UP WITH THIS IDEA SMART CITIES?

- The first smart city was arguably Amsterdam with the creation of a virtual digital city in 1994. Things then speeded up in mid-2000s when **IBM and Cisco** launched separate initiatives.

BASIC IDEA ON SMART CITY

- Click here

WHAT IS SMART CITY?

- A "smart city" is an urban area that uses Internet of Things (IoT) and information and communication technology (ICT) to deliver usable data for efficient resource and asset management. This includes information gathered from people and mechanical devices that is then processed and analyzed to track and manage power plants, water supply networks, waste disposal, traffic and transportation systems, etc.

CONTD…

- A Smart City is a place where people living in that city can enjoy the best life qualities.
- A Smart City has basic infrastructure, uses “ smart “solutions to make infrastructure and services better and relies on Area based development.
- The main Objectives of Smart City are to provide basic infrastructure, Quality of life, Clean and sustainable environment by applying smart solutions.

- The smart city, also known as an eco-city or a sustainable city, strives to raise the standard of urban services while cutting expenses. It is distinctive for its unique features, including smart governance, environment, mobility, living, and a smart economy. Their fundamental objective is to balance technical advancement with the economic, social, and ecological issues facing cities of the future.

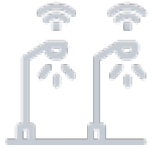
HOW DOES A SMART CITY WORK?

Smart cities utilize their web of connected IoT devices and other technologies to achieve their goals of improving the quality of life and achieving economic growth. Successful smart cities follow four steps:

- Collection
- Analysis
- Communication
- Action

SMART CITY DEVELOPMENTS

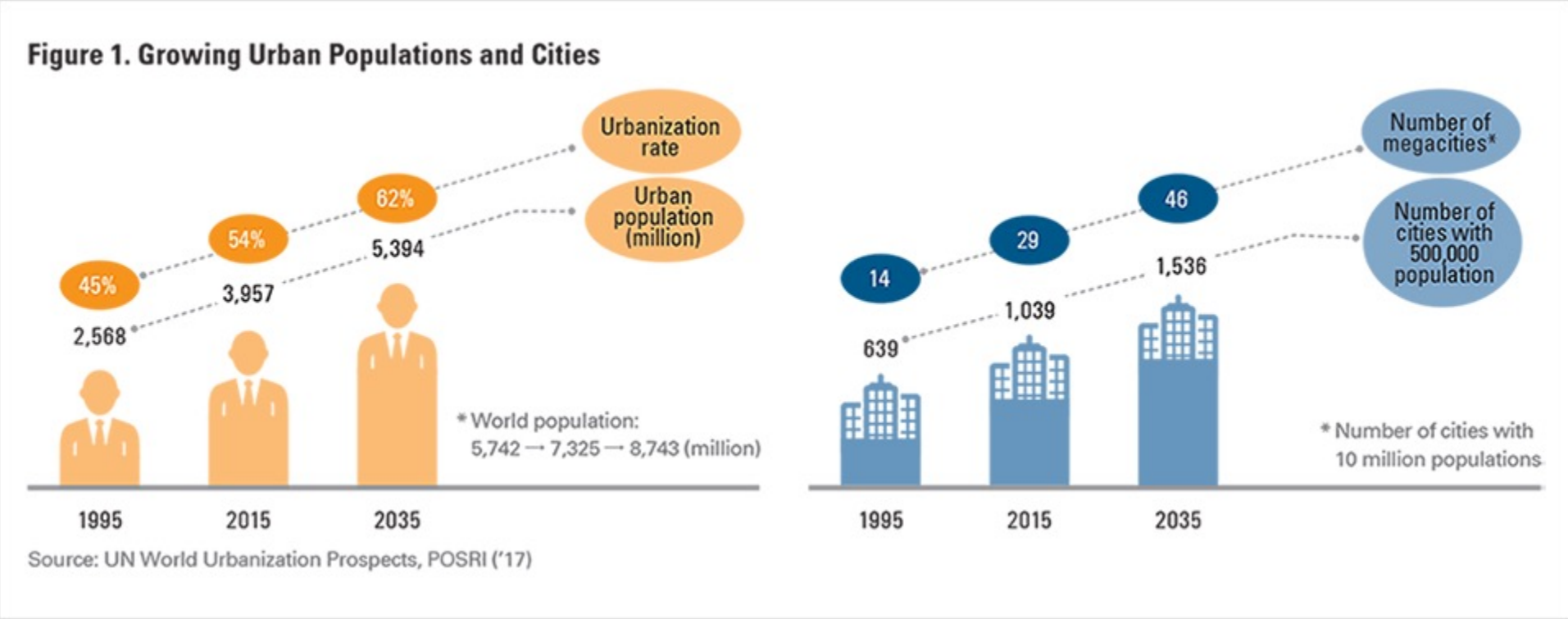
- SMART BUILDINGS
- SMART MOBILITY
- SMART LIGHTING
- SMART ROADS



SMART CITY CHARECTERISTICS

- HETEROGENEITY
- RESOURCE CONSTRAINTS
- USER INVOLVEMENT
- CONNECTIVITY AND SCALABILITY
- MOBILITY

WHY DID SMART CITIES CAME INTO PICTURE



- Urbanization has been progressing rapidly worldwide. Increasing numbers of people are moving from rural to urban areas. The global share of the urban population is expected to rise to *62%* by *2035*, up from *45%* in *1995*.
- Since manufacturing, consumption, education, and cultural development can all occur in one location, large concentrated cities are advantageous from an economic efficiency and effectiveness standpoint. Because of this, urbanization has been a common solution in many industrialized nations as a way to boost investment returns and find talent. The quality of life for city inhabitants is now threatened in a number of ways as a result of the growth of megacities and rising population density.

- Ironically, the industrial complexes, high-rise buildings, and transport infrastructure that were intended to increase public convenience have triggered several issues such as excessive energy consumption, environmental pollution, public insecurity, and income disparities. This in turn has threatened the quality of life of urban dwellers and diminished the sustainability of cities. Smart cities aim to address some of the issues stemming from rapid urbanization and high population density by using scientific and information technology to forge a more sustainable urban environment.

WHY DO WE NEED SMART CITIES?

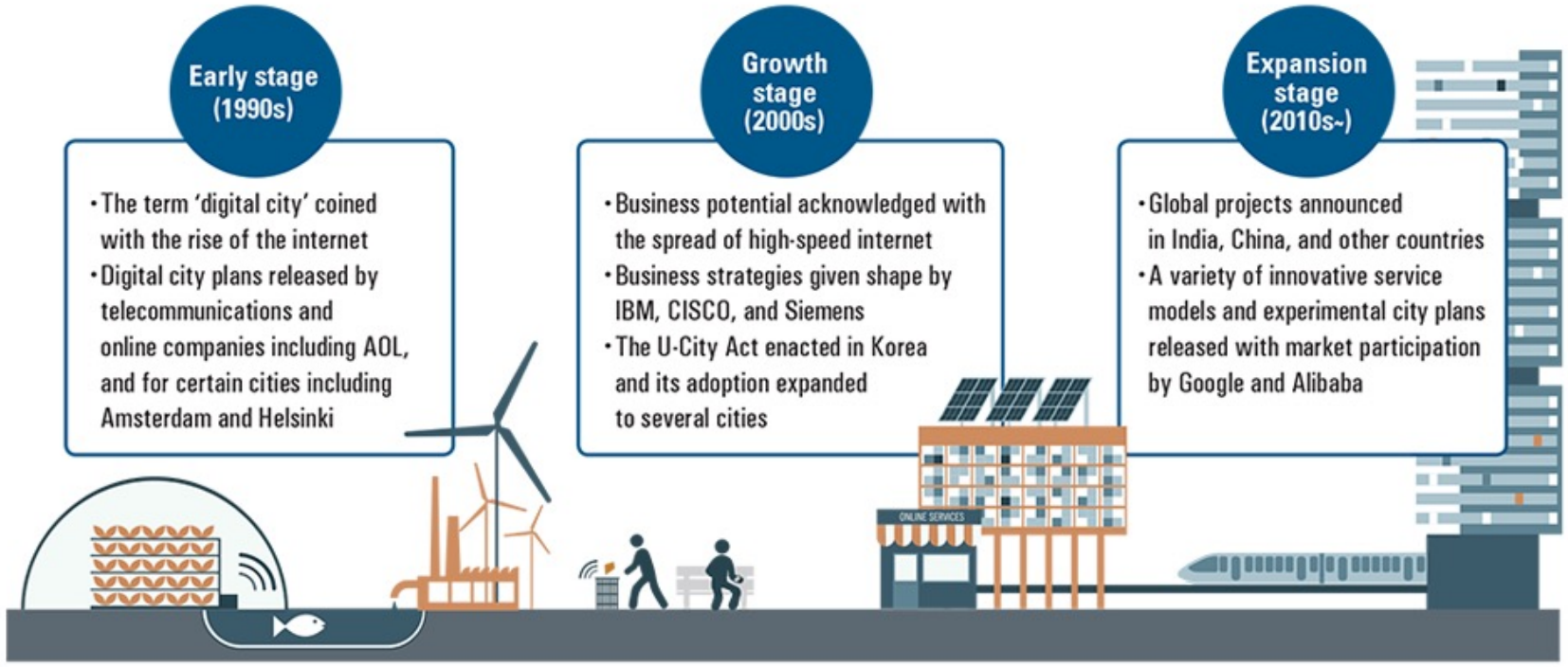
- Reduced Public spending
- Increased efficiency
- Decision making support
- Promoting innovation
- Real life information provided

- **Good infrastructure** – The main aim of constructing a smart city is to provide good infrastructure to the residents, such as water and sanitation services, *24*7* electricity supply etc.
- **Smart solutions** – Smart cities are required as it would also provide smart solutions such as providing public data, electronic service delivery, *100%* treatment of water waste, monitoring water quality etc.
- **Promotes development** – Smart cities enhance the developmental activities of a region. A lot of developmental activities such as building schools, organizations, shopping malls can take place. These activities benefit everybody including citizens, businesses, government and environment.

- **Housing for All** – The main aim of a smart city is "*housing for all*". Due to the rising urbanization, a better standard of living is required. To support this rising shift, a sustainable model of housing should be developed.
- **Provides employment** – A smart city is an economy of agglomeration. It provides various opportunities and advantages to its residents. India is expanding rapidly, and the emergence of smart city can provide employment for many. The construction of a smart city requires a lot of manpower

EVOLUTION OF SMART CITY

Figure 2. Development Stages of Smart Cities



Source: Weekly KDB Report ('18) edited by POSRI

BENEFITS OF SMART CITIES

Environmental impact

- Reducing the CO2 footprint is the main driver behind the development of smart and sustainable cities. Improving energy efficiency and storage, waste management, traffic conditions are among the greatest advantages.

Optimized energy & water management

- Smart grids and smart water management are recurring themes of smart cities. Energy consumption and potable water monitoring ensure the availability of energy and the quality of tap water across the city.

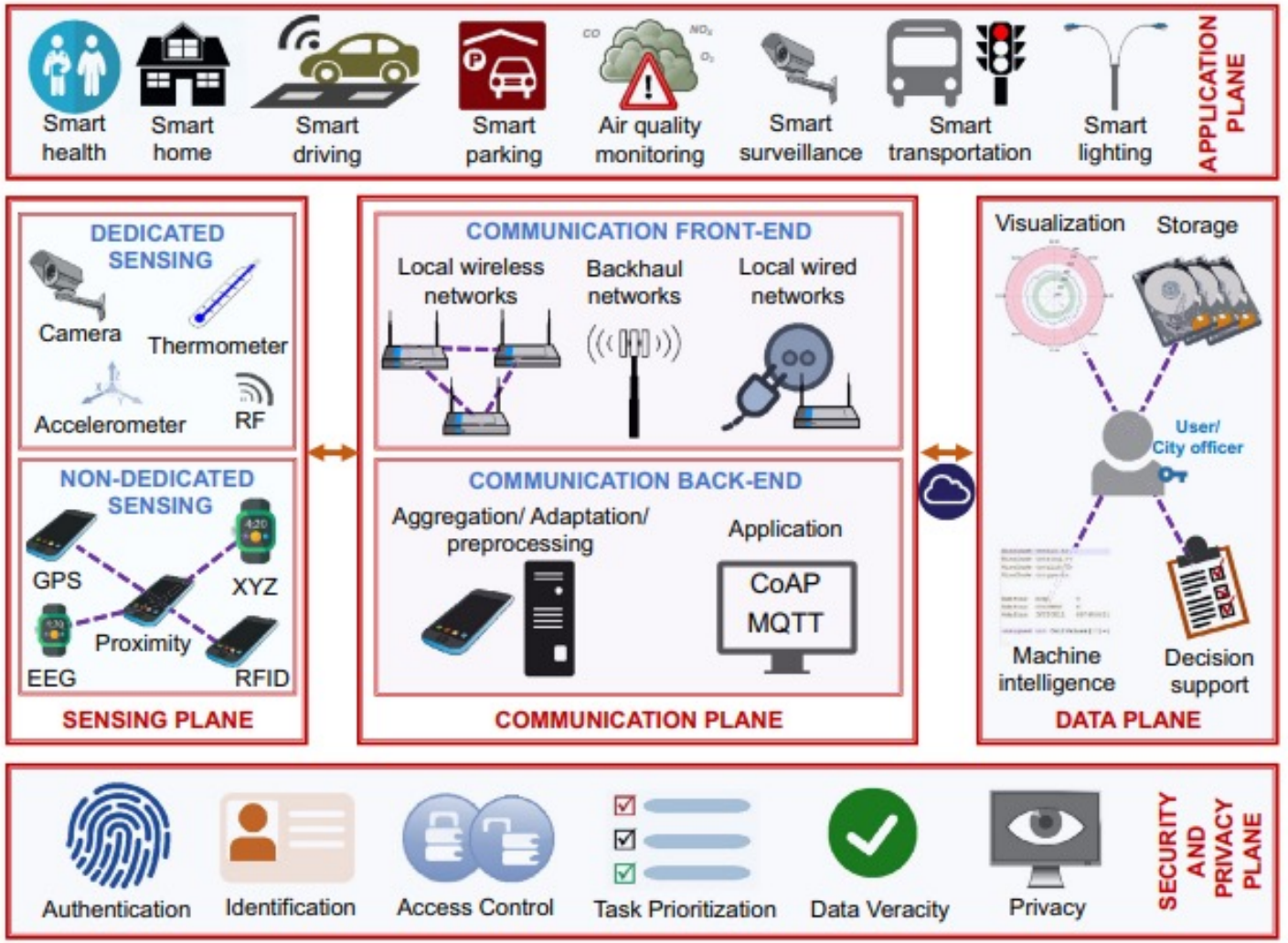
Transportation

- Clean and efficient transportation of goods, services and people is essential. In the hope of optimizing mobility, many cities are turning to smart technologies to ease traffic congestion and provide users with real-time updates.

Security

- Safety is a priority for all cities. The accelerated development of smart cities should allow municipalities to better monitor their citizens thanks to CCTV cameras with facial recognition. In addition, state-of-the-art CCTV cameras are also equipped with motion and smoke detectors, as well as fire alarms.

ARCHITECTURE OF SMART CITY



CONCEPTS OF SMART CITY

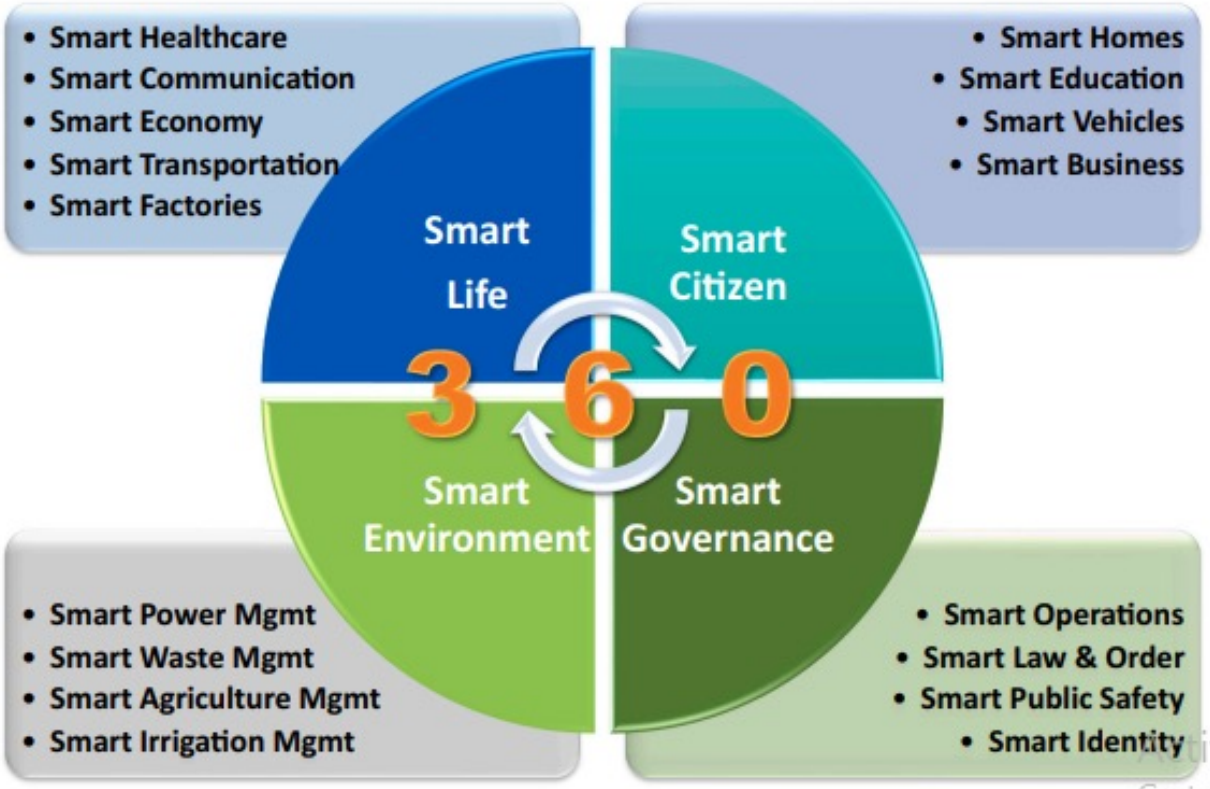
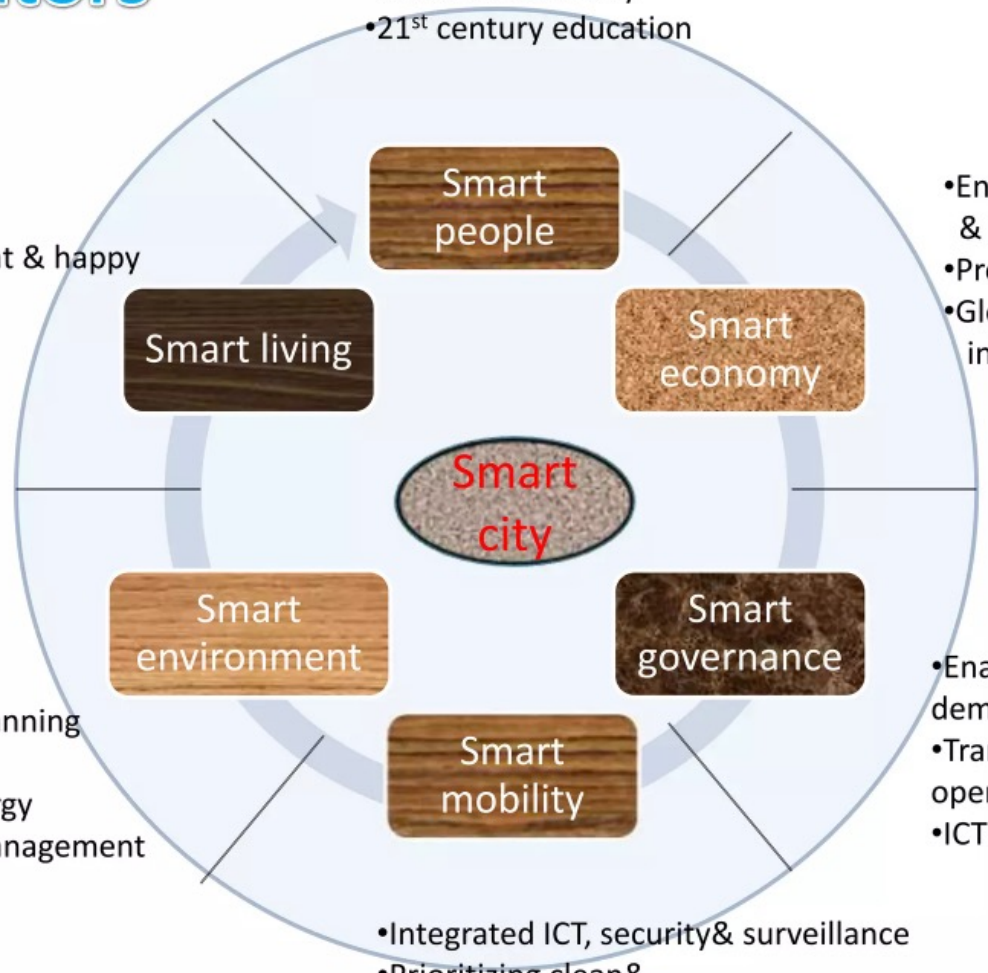


Fig. 1. 360 degrees of smartness in smart city - a system-of-systems approach.

Indicators



•Inclusive society
•Embrace creativity
•21st century education

•Entrepreneurship & innovations
•Productivity
•Global & local interconnectedness

•Enabling supply & demand side policy
•Transparency & open data
•ICT & E-Governance

•Integrated ICT, security& surveillance
•Prioritizing clean& non motorized options
•Mixed-modal access, SPV's

•Green buildings
•Green urban planning
•Green energy
•Renewable energy
•Waste water management
•sanitation

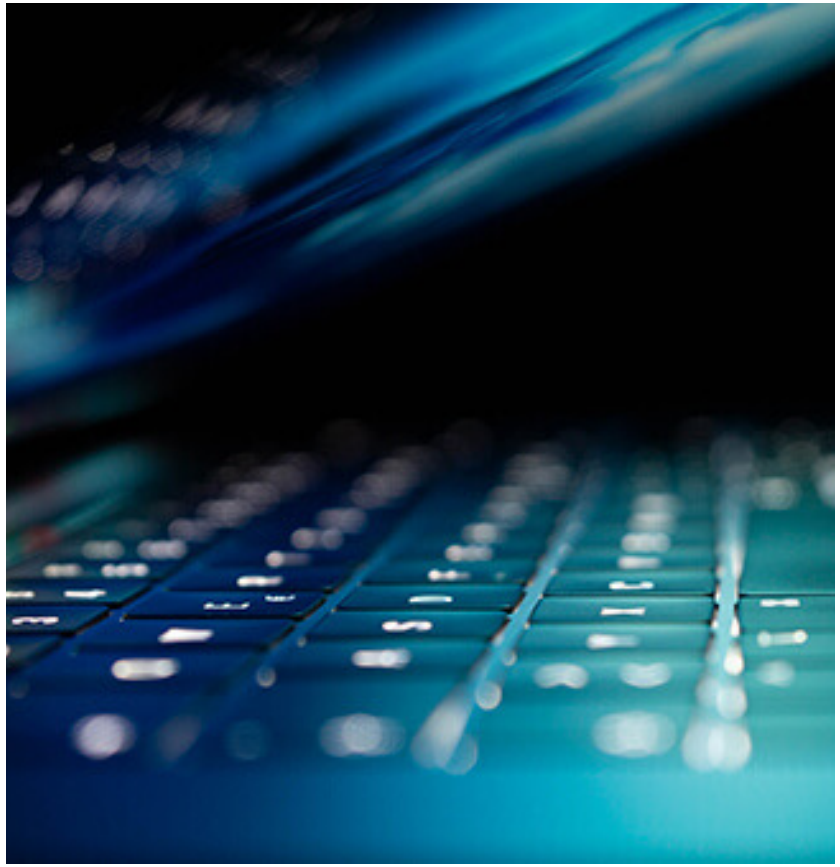
•Safe
•Healthy
•Culturally vibrant & happy

CHALLENGES

- **INFRASTRUCTURE AND COSTS**
- Smart cities use sensor technology to gather and analyze information such as rush hour stats, air quality or crime rates. The implementation of these sensors requires a sophisticated and costly infrastructure.

SECURITY AND PRIVACY CONCERNS

- Even though security is part of the benefits, it can also be regarded as a challenge as the use of IoT and sensor technology increases. In fact, the threat of cyber attacks is a critical issue for smart cities. Also, to avoid concerns about data use, smart cities need to involve their citizens.
- Awareness, education, and transparency on the purpose of data collection are crucial to make the community feel that they are truly taking part in making their city more sustainable.



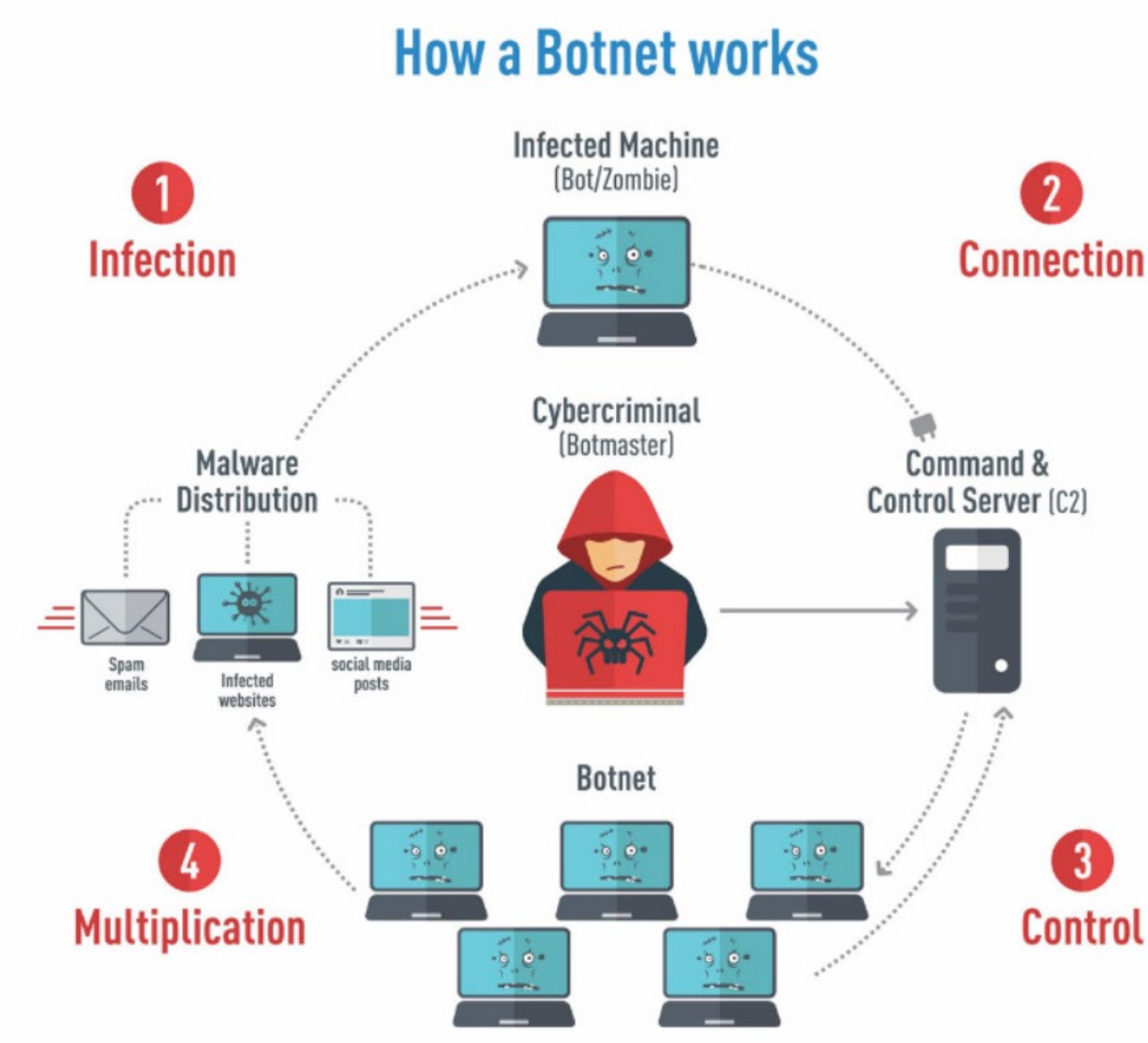
SOCIAL RISKS

- Inclusive urbanization must be a priority to deal with the increasing vulnerability of poor and slum populations. That is why we need to ensure that no population is excluded from smart city data collection and use.

SECURITY CHALLENGES IN SMART CITIES

Botnet Activities In IoT-based Smart Cities

- Botnet is a group of hacked computers, smart appliances and Internet-connected devices.
- Botnet, which can infect devices such as webcams, printers, DVRs, and routers, etc. and spread infection to many heterogeneous IoT devices which finally result a DDoS against target servers.
- Devices that are designed with low security or no security at all can be affected by a Botnet.


How a Botnet works
1
Infection
Infected Machine
(Bot/Zombie)
2
Connection
Cybercriminal
(Botmaster)
Malware
Distribution
Command &
Control Server (C2)
Spam
emails
Infected
websites
social media
posts
Botnet
4
Multiplication
3
Control

THREATS OF SELF-DRIVEN CARS IN SMART CITIES

- Many Tech companies have spent huge amount of money in developing autonomous vehicles (AVs), aiming to reduce traffic accidents and to build a cleaner and smarter society.
- This rapid growing in developing and using AVs has seen as a major security issue because once an AV is hacked, both life safety and data privacy of a person will be threatened.
- The hackers can embed security bugs to conduct remote attacks, such as applying the brakes, shutting down the engine and controlling the steering, signal jumps.
- Besides this, massive personal data collected by the computer system of a self-driving vehicle may cause significant privacy issues.

PRIVACY ISSUES OF VIRTUAL REALITY IN SMART CITIES

- In smart cities, virtual reality (VR) has been embraced by various organizations such as city planning departments, healthcare service providers, engineering industry sector, administration sector, etc.
- The sensitive information captured by VR technology in developing a smart city is shared with third parties, unencrypted communications between VR devices, and the data stored by sensors all pose threats of privacy leakage.
- Application of VR in Smart Cities is as follows;
  - Urban Planning
  - Emergency Management
  - Educational Training
  - Culture and Tourism in smart cities
  - Medical Analysis

THREATS POSED BY AI IN SMART CITIES

- AI systems play indispensable roles in various smart applications, such as automatic control of trading systems, home appliances, pacemakers, continuous glucose monitoring systems, etc.
- Issues of AI in smart cities are
  - Smart Traffic Control Failure
  - Object Detection
  - Speech Recognition
  - Face Recognition

SECURITY REQUIREMENTS

- Authentication And Confidentiality.
- Availability And Integrity.
- Lightweight Intrusion Detection and Prediction
- Privacy Protection Terminologies which include
  - Cryptography
  - Blockchain
  - Biometrics
  - Machine Learning and Data Mining

CRYPTOGRAPHY

- Cryptographic algorithms are the backbone of security and privacy protection for the services of smart applications because they avoid the access of distrusted parties during the data life circle of storing, processing and sharing.
- Traditional encryption algorithms are not completely suitable for resource-constrained devices because of their computational complexity and energy consumption. So, lightweight encryption techniques are applied.
- Popular cryptographic algorithms used are;
  - AES (Advance Encryption Standard)
  - Homomorphic Encryption
  - DES (Data Encryption Standard)

BLOCKCHAIN

- Blockchain is one such technology essential to create more secure, transparent, efficient and resilient cities.
- Uses of blockchain in smart cities;
  - Increased Cybersecurity
  - Enhanced Healthcare
  - Better Waste Management System
  - Increased Energy Savings
  - Simplified Learning
  - Efficient Mobility

BIOMETRICS

- In IoT-based systems, biometrics are widely for authentication.
- This technology can be used to automatically recognize a person through unique behavioral and biological characteristics. The bio-data are extracted from fingerprints, faces, voices, handwritten signatures.
- Biometric methods that could be employed in smart cities are
  - Facial Recognition
  - Age Estimation and Gender Detection
  - Gait Recognition
  - Expression, Emotion and Sentiment Recognition
  - Finding Missing people

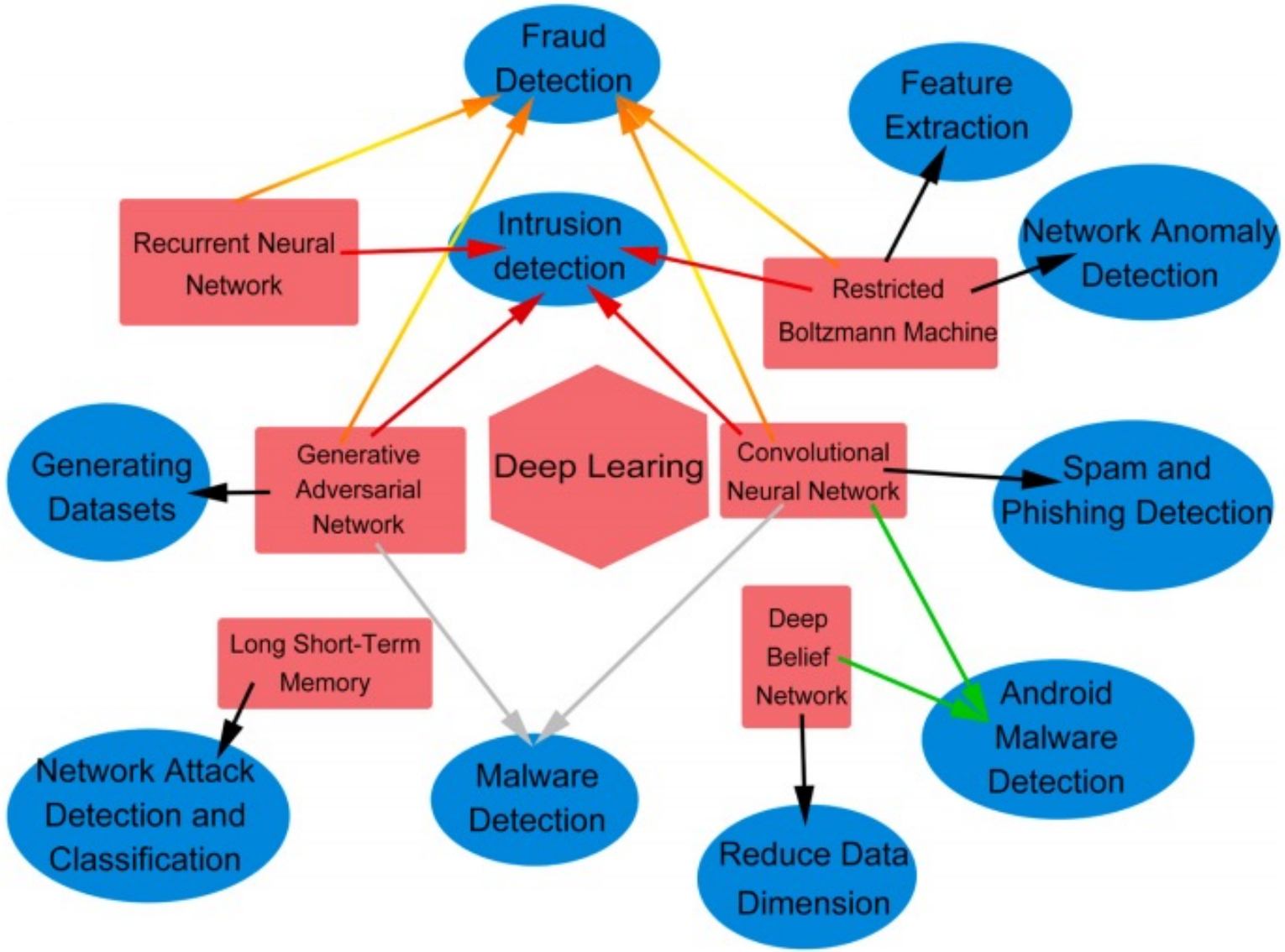
MACHINE LEARNING AND DATA MINING

- Machine Learning have been employed specially to improve the efficiency of intrusion detection systems in smart cities.
- Applications of ML and Data Mining in smart cities include;
  - Novel feature extraction and selection model to detect attacks in Wi-Fi networks, which has a high detection rate.
  - User-centric ML technologies to predict and make personalized decisions.
  - SVM to design a multi sensor-based authentication system for smartphone users.
  - Machine learning models to detect and prevent intrusions in Wireless Sensor Networks.
  - Determining new regulations and information to provide better services from large amount of data collected by many sensors and devices around consumers.

APPLICATIONS AND CASE STUDIES FOR CYBER SECURITY IN SMART CITIES

Intrusion Detection

- There are numerous sorts of inquire about on interruption location based on DL, basically choosing CNN and RNN. Lin, Lin, Wang, Wu, and Tsai *(2018)* utilized a strategy based on the LeNet-5 show to conduct cyber interruption discovery. In this try, the number of preparing tests surpassed *10,000*, and the precision of interruption location come to *99.65%*, and the in general exactness was *97.53%*. Dong, Wang, and He *(2019)* proposed a real-time cyber interruption discovery framework, which utilized the CNN strategy of the programmed encoder AlexNet demonstrate (AE-Alexnet), and the discovery rate exactness of the interruption location KDD99 dataset *(Glass, 2007)* was as tall as *94.32%*. Khan, Zhang, Alazab, and Kumar *(2019)* proposed the cyber interruption location show of the progressed CNN calculation and assessed the execution of the moved forward CNN demonstrate and DBN demonstrate within the KDD99 dataset *(Glass, 2007)*, the test comes about appeared the improved CNN show has an exactness of *99.23%*, which is prevalent to the DBN.


Fraud Detection
Feature Extraction
Recurrent Neural Network
Intrusion detection
Network Anomaly Detection
Restricted Boltzmann Machine
Generating Datasets
Generative Adversarial Network
Deep Learing
Convolutional Neural Network
Spam and Phishing Detection
Long Short-Term Memory
Deep Belief Network
Android Malware Detection
Network Attack Detection and Classification
Malware Detection
Reduce Data Dimension

- In expansion, Alom and Taha *(2017a)* conducted an curiously study in which they combined profound learning strategies and neuromorphic computing frameworks for cyber interruption discovery, the combination of utilizing KDD99 dataset *(Container, 2007)* to assess the modern strategy on IBM's Genuine North neurosynaptic processor, the exploratory comes about appeared around *90.12%* precision for cyber interruption discovery for cyber security when utilizing *20,000* preparing tests and have realized the application of moo control utilization, with less than *50.036* computation control.

- The portable gadget working framework Android discharged by Google, because of its openness and flexibility, endless noxious computer program too exists in Android generous applications. Android malware harm has increased drastically due to clashes of intrigued over the past few years, and this exceptional issue concerns the social and organizational aspects of keen cities (Fard, Karimimpour, Dehghantanha, Jahromi, & Srivastava, 2020). Numerous DL strategies for ensuring the Android system are presented by Sabhadiya, Barad, and Gheewala *(2019)*, and different android malware discovery innovations based on DL are dis_x0002_cussed, counting Maldozer, DroidDetector, DroidDeepLearner, Deep_x0002_Flow, Droid Delver, and DroidDeep. Karbab, Debbabi, Derhab, and Mouheb *(2018)* displayed MalDozer, an programmed Android malware detection and family attribution system system based on CNN. MalDozer can convey on versatile and IoT gadgets, the creators conducted several tests on MalDozer based on the changes within the amount of malware within the dataset. The F1 score extend is *96–99%*, and the untrue positive rate extend is *0.06–2%*. Vinayakumar, Soman, Poornachandran, and Sachin Kumar *(2018)* utilized LSTM systems to distinguish and classify Android malware. Through a huge number of tests, they indi_x0002_cated that the arrange seem distinguish and classify Android malware with high exactness, and LSTM may be reasonable for recognizing and classifying malware and typical program. Xiao *(2019)* presented a malware detection strategy based on CNN, which can be specifically learned from Dalvik bytecode. The normal location time of the demonstrate was *0.22* seconds, and the in general exactness of the demonstrate come to more than *93%*.

- In expansion, Alom and Taha *(2017a)* conducted an curiously study in which they combined profound learning strategies and neuromorphic computing frameworks for cyber interruption discovery, the combination of utilizing *KDD99* dataset *(Container, 2007)* to assess the modern strategy on IBM's Genuine North neurosynaptic processor, the exploratory comes about appeared around *90.12%* precision for cyber interruption discovery for cyber security when utilizing *20,000* preparing tests and have realized the application of moo control utilization, with less than *50.036* computation control.and profound learning(GDMC) proposed by Gibert, Mateu, Planes, and Vicens *(2019)*, and it does not depend on the pre-trained demonstrate. Vinayakumar, Alazab, Jolfaei, Soman, and Poornachandran *(2019)* collected malware tweets from *2010* to *2017* on Twitter and analyzed *25* families of ransomware, of which *67%* of information was utilized for preparing and *33%* of information was utilized for testing, where the DNN can successfully classify ransomware tweets to their comparing family, and this proposed method can be utilized to ceaselessly screen online posts in social media information.

SPAM DETECTION

- Spam location Spam alludes to spontaneous emails with partitioned purposes, as savvy cities progress our lives, we are progressively helpless to the perpetual threat of spam. Bosaeed, Katib, and Mehmood *(2020)* submitted a sys_x0002_tem for recognizing brief message benefit (SMS) spam on versatile gadgets. The framework comprises of three machine learning (ML) classifiers: Naïve Bayes (NB), Back Vector Machine (SVM), and Naïve Bayes Multino_x0002_mial (NBM), 5 channels. The try was carried out on the Android mobile stage and the server. Particularly, the creators compared the SVM classifier on *5* channels (PF1, PF2, PF3, PF4, PF5) on the preprocessing and exactness result of include extraction, they found that the PF5 channel and SVM performed best in classifying SMS messages. The utilize of profound learning to distinguish spam is additionally picking up notoriety. For occasion, Chetty, Bui, and White *(2019)* proposed a spam detection model. This demonstrate could be a combination of word inserting innovation and neural organize word embedding technology and neural network algorithm, and its performance increases with the increase of data volume. However, the experiment found that the false positives (FP) increased they evaluated the performance of SVM, CNN, and multi-layer percep_x0002_tron (MLP) for distinguishing spam images from ham images, experi_x0002_ments showed that CNN is especially suitable for detecting spam images, accuracy is as high as *99.02%*, at the same time, the authors pointed out that RNN and LSTM may also be helpful for image spam research.

FRAUD DETECTION

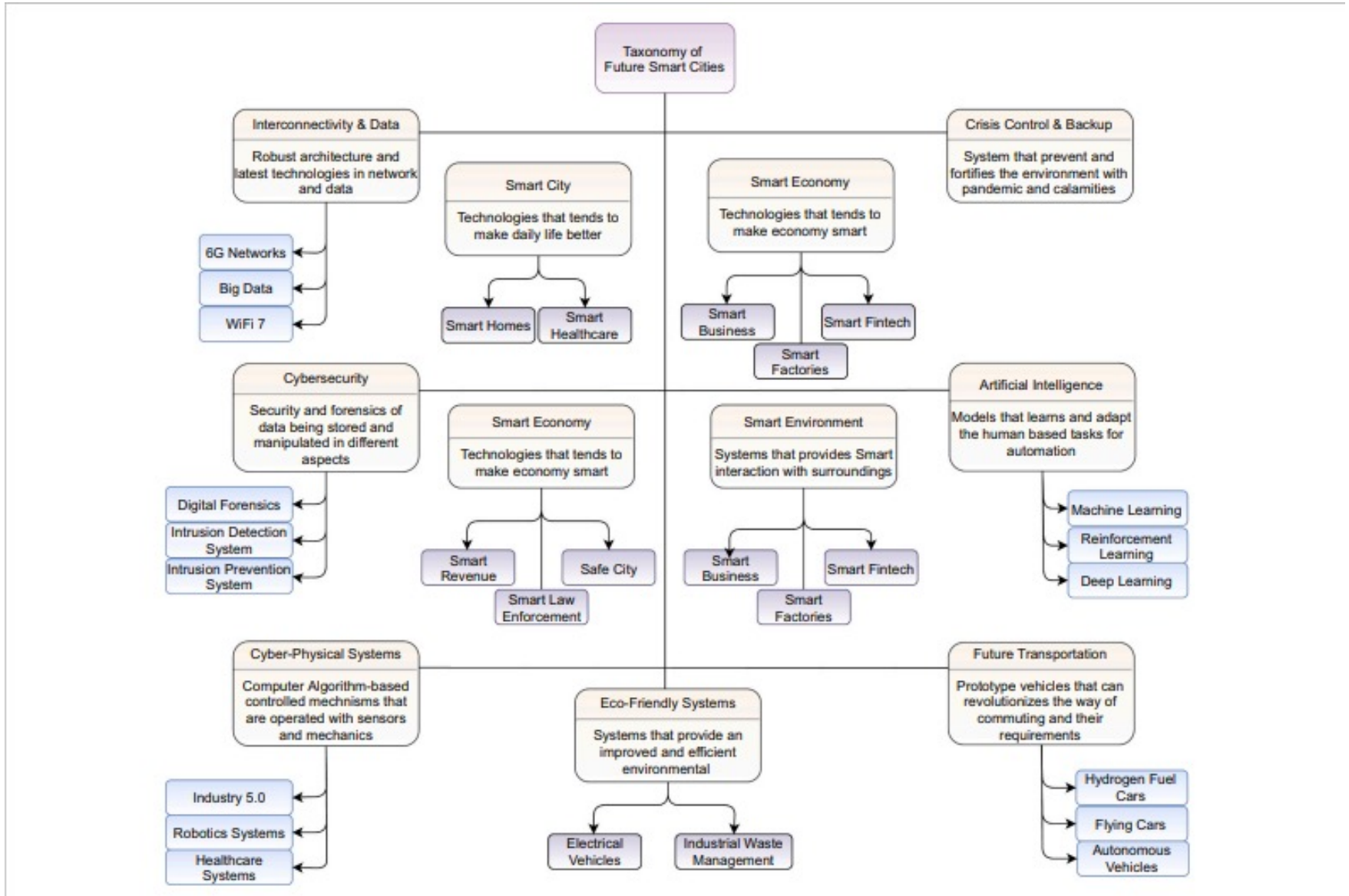
- Financial development promotes urban economic growth to a certain extent, and the development of the financial sector should also become one of the missions of smart cities *(Arora, 2018)*. Fraud is domain-specific *(Mojtahed, 2019)*, in the financial field, cyber attacks mainly focus on financial and reputation problems caused by fraud and data leakage, and credit fraud often causes huge losses in the financial field. Sadiq, Faris, Ala'M, Mirjalili, and Ghafoor *(2019)* proposed an innovative fraud detection model based on the feature extraction method to accurately identify the source of fraud in e-commerce to prevent further fraud. This model uses the SVM to construct the classi_x0002_fier, a multi-node optimizer for fraudulent feature extraction. Zheng, Zhou, Sheng, Xue, and Chen *(2018)* introduced the GAN-DAE model, which can effectively detect fraudulent online transfers without a large amount of training data.

CHALLENGES AND FUTURE DIRECTION

- IoT-based Network Security In Smart Cities
- Security And Privacy Issues In Fog-based System
- User-centric And Personalized Protection Method
- Data Minimization Towards Smart Application
- Lightweight Security Solutions
- Theoretical Complement

FUTURE WORK AND CONCLUSION

- **Scalability**: Better scalability also ensures that a product can provide more features to consumers. The more features in the product also save the cost being spent on other items and enhance the usability of the product
- **Fast deployment**: The design of the technology plays a crucial role in managing the space and deployment of the technology. In the modern era of technology, sustainable but portable deployment is preferred since it takes less time in implementation with less workforce.
- **Eco friendly and efficiency**: The fundamental source of power is the electricity that most technologies consume. However, the source of power can be based on multiple fuels.


Taxonomy of Future Smart Cities
Interconnectivity & Data
Robust architecture and latest technologies in network and data
6G Networks
Big Data
WiFi 7
Smart City
Technologies that tends to make daily life better
Smart Homes
Smart Healthcare
Smart Economy
Technologies that tends to make economy smart
Smart Business
Smart Fintech
Smart Factories
Crisis Control & Backup
System that prevent and fortifies the environment with pandemic and calamities
Cybersecurity
Security and forensics of data being stored and manipulated in different aspects
Digital Forensics
Intrusion Detection System
Intrusion Prevention System
Smart Economy
Technologies that tends to make economy smart
Smart Revenue
Safe City
Smart Law Enforcement
Smart Environment
Systems that provides Smart interaction with surroundings
Smart Business
Smart Fintech
Smart Factories
Artificial Intelligence
Models that learns and adapt the human based tasks for automation
Machine Learning
Reinforcement Learning
Deep Learning
Cyber-Physical Systems
Computer Algorithm-based controlled mechnisms that are operated with sensors and mechanics
Industry 5.0
Robotics Systems
Healthcare Systems
Eco-Friendly Systems
Systems that provide an improved and efficient environmental
Electrical Vehicles
Industrial Waste Management
Future Transportation
Prototype vehicles that can revolutionizes the way of commuting and their requirements
Hydrogen Fuel Cars
Flying Cars
Autonomous Vehicles

Further reference

Want to know about smart city more?

THANK YOU