Cyber Security Threats: A risk Management approach to Smart Cities of Pakistan

By

JUNAID AHMED KHAN

(Registration No. 00000326429)

DEPARTMENT OF CYBER SECURITY

PAKISTAN NAVY ENGINEERING COLLEGE (PNEC)

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY (NUST)

ISLAMABAD, PAKISTAN

(2024)

Cyber Security Threats: A risk Management approach to Smart Cities of Pakistan

By

JUNAID AHMED KHAN

(Registration No. 00000326429)

A Thesis submitted to National University of Science and Technology, Islamabad

in partial fulfillment of the requirements for the degree of

Masters of Science in Cyber Security

Thesis Supervisor:

CDRE DR NADEEM KURESHI

DEPARTMENT OF CYBER SECURITY

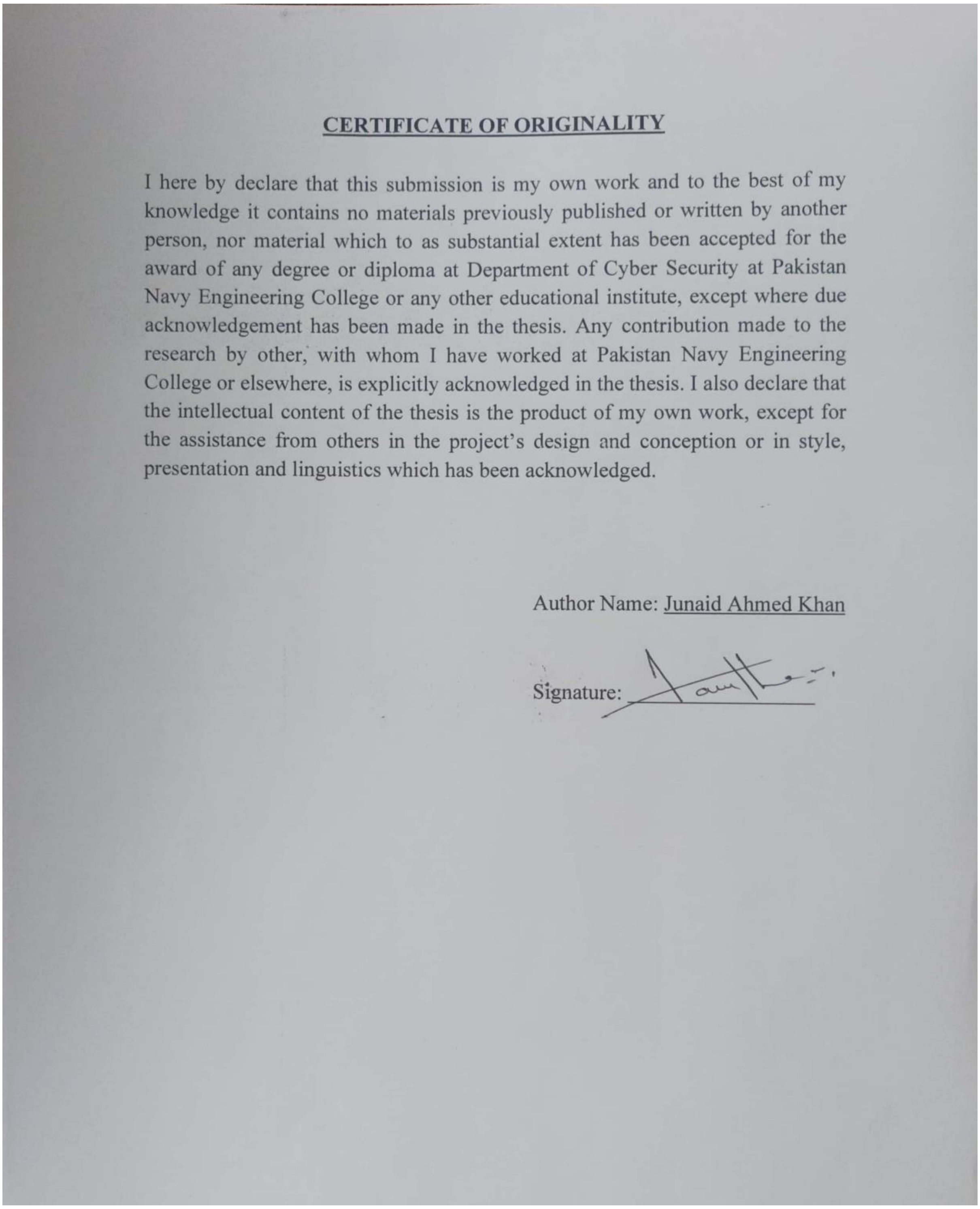
PAKISTAN NAVY ENGINEERING COLLEGE (PNEC)

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY (NUST)

ISLAMABAD, PAKISTAN

(2024)

CERTIFICATE OF ORIGINALITY



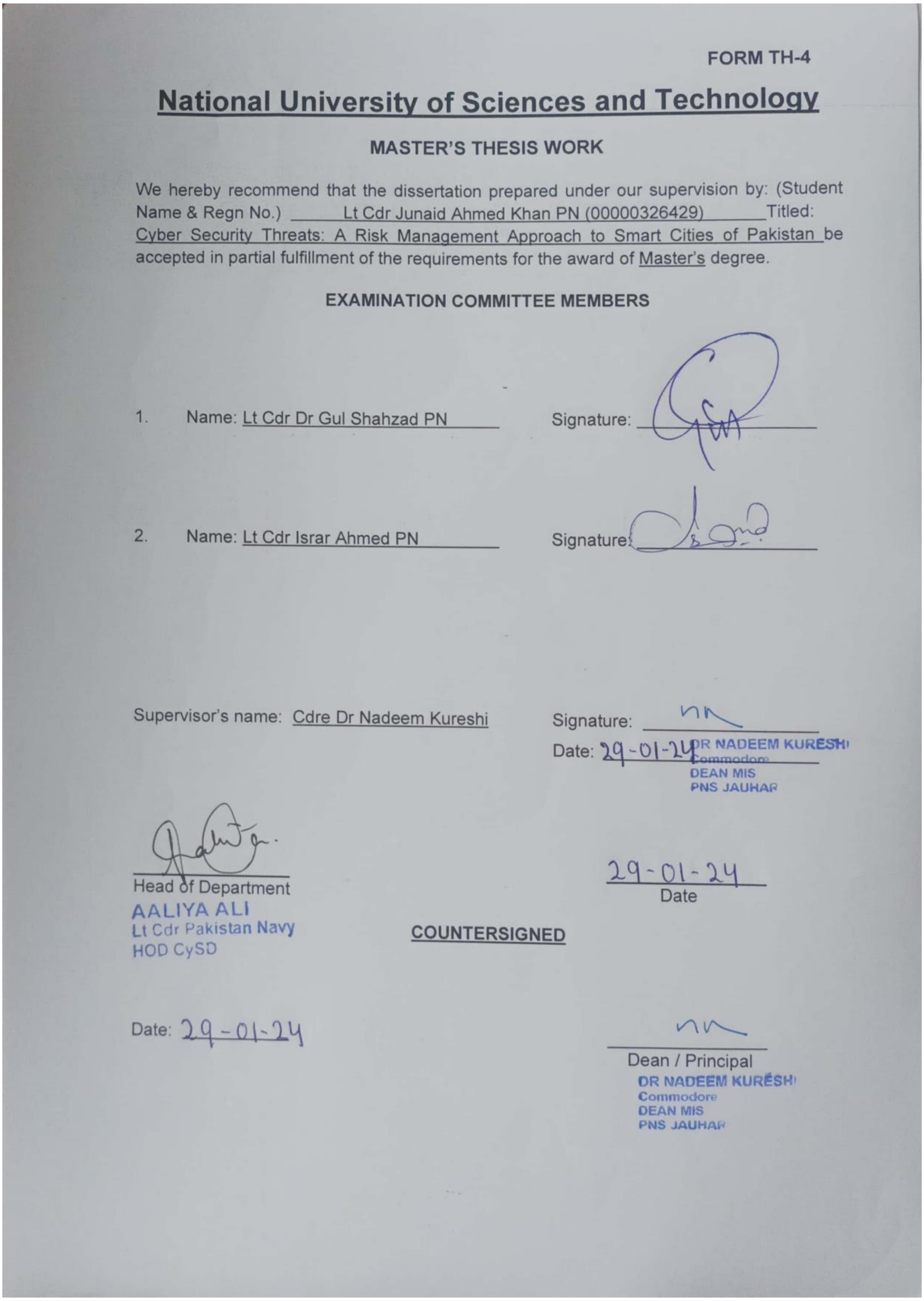
CERTIFICATE OF ORIGINALITY

I here by declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to as substantial extent has been accepted for the award of any degree or diploma at Department of Cyber Security at Pakistan Navy Engineering College or any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by other, with whom I have worked at Pakistan Navy Engineering College or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of the thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: Junaid Ahmed Khan

Signature: ______________

FORM TH-4



FORM TH-4

National University of Sciences and Technology

MASTER'S THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Regn No.) Lt Cdr Junaid Ahmed Khan PN (00000326429) Titled: Cyber Security Threats: A Risk Management Approach to Smart Cities of Pakistan be accepted in partial fulfillment of the requirements for the award of Master's degree.

EXAMINATION COMMITTEE MEMBERS

1. Name: Lt Cdr Dr Gul Shahzad PN Signature:

2. Name: Lt Cdr Israr Ahmed PN Signature:

Supervisor's name: Cdre Dr Nadeem Kureshi Signature:

Date: 29-01-24

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

Head of Department

AALIYA ALI
Lt Cdr Pakistan Navy
HOD CySD

29-01-24
Date

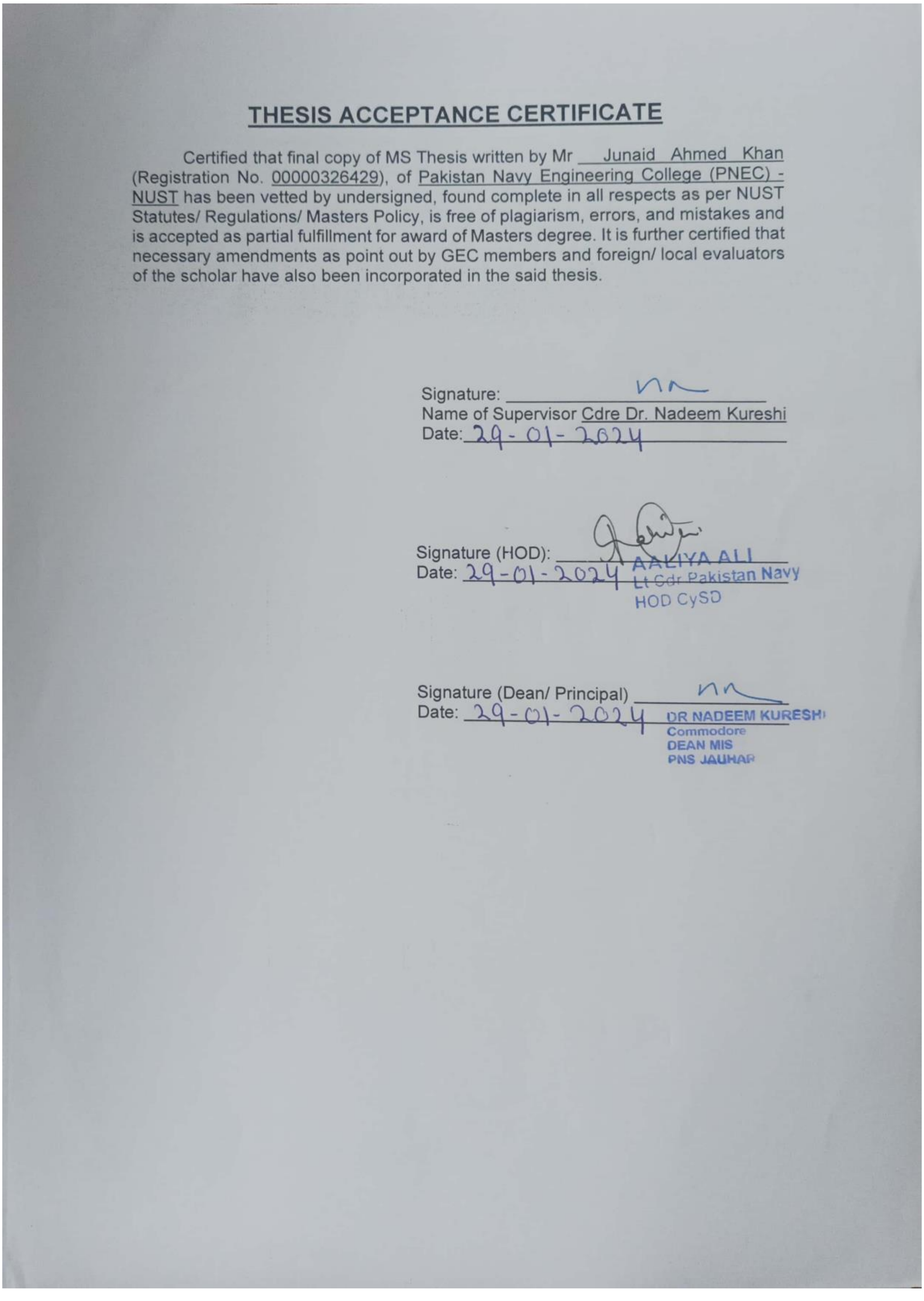
COUNTERSIGNED

Date: 29-01-24

Dean / Principal

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

THESIS ACCEPTANCE CERTIFICATE



THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Mr Junaid Ahmed Khan (Registration No. 00000326429), of Pakistan Navy Engineering College (PNEC) - NUST has been vetted by undersigned, found complete in all respects as per NUST Statutes/ Regulations/ Masters Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of Masters degree. It is further certified that necessary amendments as point out by GEC members and foreign/ local evaluators of the scholar have also been incorporated in the said thesis.

Signature: ______________________
Name of Supervisor Cdre Dr. Nadeem Kureshi
Date: 29-01-2024

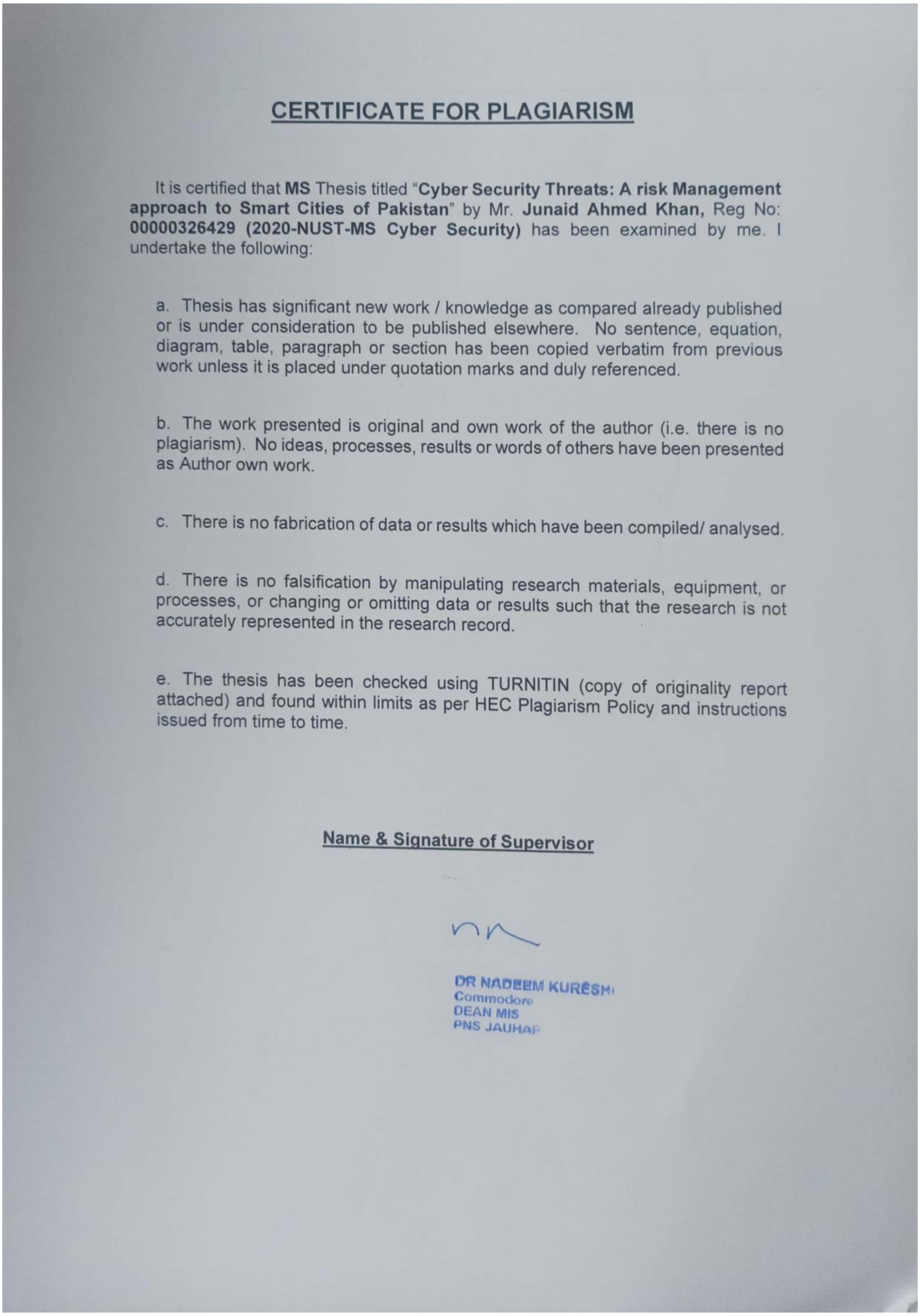
Signature (HOD): ______________________
Date: 29-01-2024

AALIYA ALI
Lt Cdr Pakistan Navy
HOD CySD

Signature (Dean/ Principal) ______________________
Date: 29-01-2024

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

CERTIFICATE FOR PLAGIARISM



CERTIFICATE FOR PLAGIARISM

It is certified that **MS** Thesis titled "**Cyber Security Threats: A risk Management approach to Smart Cities of Pakistan**" by Mr. **Junaid Ahmed Khan,** Reg No: **00000326429 (2020-NUST-MS Cyber Security)** has been examined by me. I undertake the following:

a. Thesis has significant new work / knowledge as compared already published or is under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.

b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.

c. There is no fabrication of data or results which have been compiled/ analysed.

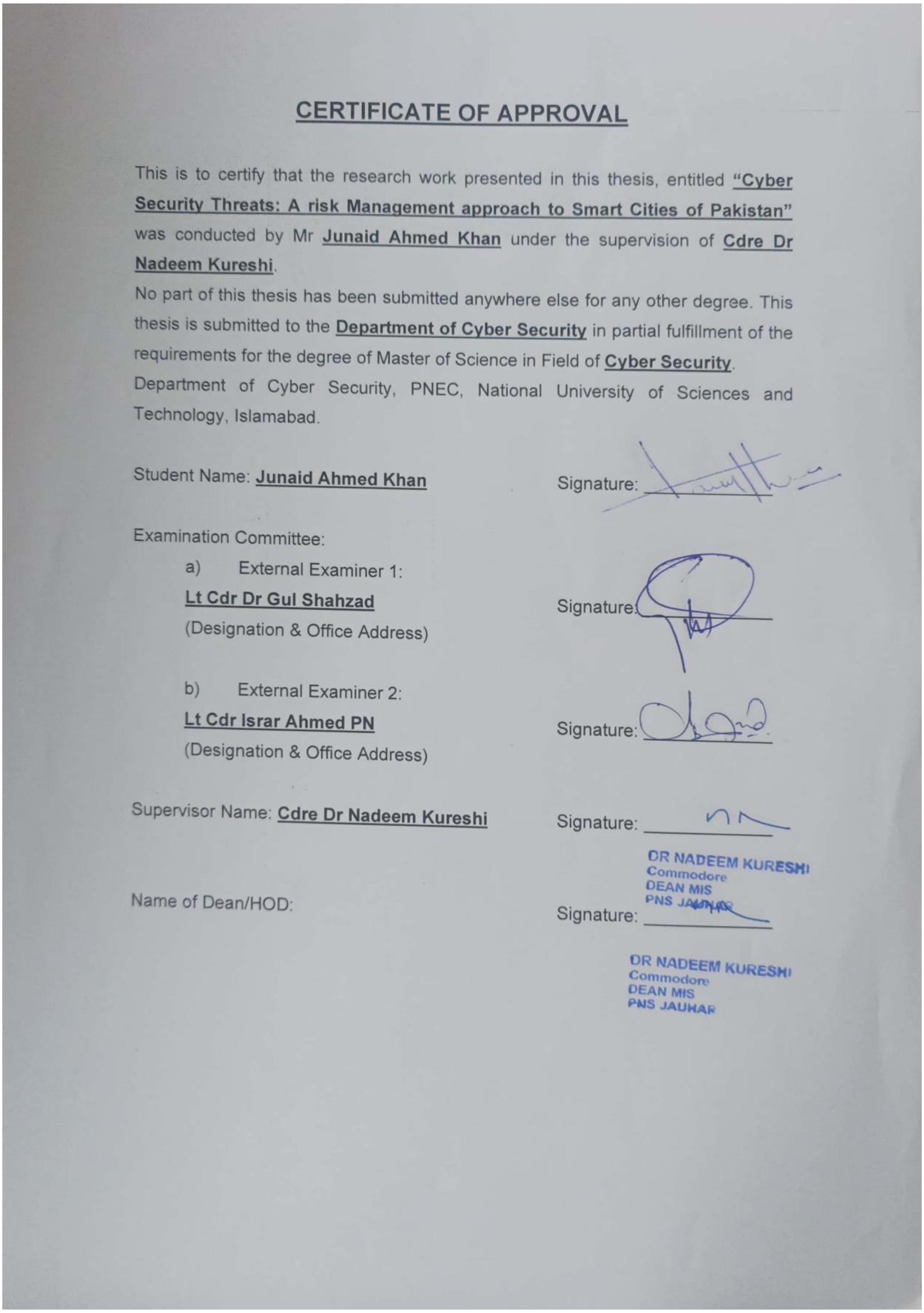
d. There is no falsification by manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.

e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC Plagiarism Policy and instructions issued from time to time.

Name & Signature of Supervisor

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

CERTIFICATE OF APPROVAL



CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled **"Cyber Security Threats: A risk Management approach to Smart Cities of Pakistan"** was conducted by Mr **Junaid Ahmed Khan** under the supervision of **Cdre Dr Nadeem Kureshi**.

No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Department of Cyber Security** in partial fulfillment of the requirements for the degree of Master of Science in Field of **Cyber Security**.

Department of Cyber Security, PNEC, National University of Sciences and Technology, Islamabad.

Student Name: **Junaid Ahmed Khan** Signature: ____________

Examination Committee:

a) External Examiner 1:

Lt Cdr Dr Gul Shahzad Signature: ____________

(Designation & Office Address)

b) External Examiner 2:

Lt Cdr Israr Ahmed PN Signature: ____________

(Designation & Office Address)

Supervisor Name: **Cdre Dr Nadeem Kureshi** Signature: ____________

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

Name of Dean/HOD: Signature: ____________

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

ACKNOWLEDGEMENTS

I am thankful to my Creator Allah Subhana-Watala to have guided me throughout this work at every step and for every new thought which You setup in my mind to improve it. Indeed I could have done nothing without Your priceless help and guidance. Whosoever helped me throughout the course of my thesis, whether my parents or any other individual was Your will, so indeed none be worthy of praise but You.

I am profusely thankful to my beloved parents who raised me when I was not capable of walking and continued to support me throughout in every department of my life.

I would also like to express special thanks to my supervisor Cdre Dr Nadeem Kureshi for his help throughout my thesis. I would also like to pay special thanks to Lt Cdr Qurrat Ul Ain PN for her tremendous support and cooperation. Each time I got stuck in something, she came up with the solution. Without her help I wouldn’t have been able to complete my thesis. I appreciate her patience and guidance throughout the whole thesis.

I would also like to thank Lt Cdr Dr Gul Shehzad PN and Lt Cdr Israr Ahmed PN for being on my thesis guidance and evaluation committee and express my special thanks to Lt Cdr Aliya PN for her help.

Finally, I would like to express my gratitude to all the individuals who have rendered valuable assistance to my study.

DEDICATION

Dedicated to my exceptional parents, wife and adorable daughter whose tremendous support and cooperation led me to this wonderful accomplishment.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In an effort to revolutionize people's lives, smart cities have brought about a multitude of benefits. Increased economic efficiency, cost savings, and reduced environmental impact are just a few of those. The smart city, however, is still in its early stages. *(W Strielkowski, 2020)* As a result of its reliance on technology, one of its biggest problems is cyber security, which leaves it vulnerable to cyber-attacks and illegal hacking, both of which can result in considerable losses. Apart from that, a lingering issue is a security in smart cities due to conflicting interests of various parties, a high degree of interdependence, and social and political complexity. *(U Ammara, 2022)*

The smart city is an ecosystem that provides a collection of e-services. In this metropolis, the essential infrastructures are connected to one another. *(T Campisi, 2021)* The goal of increased data sharing between municipal domains is to manage the key resources and maximize the use of technology in municipal administration, specifically to improve the quality of the dynamic services on offer. Nevertheless, there are no guidelines or benchmarks for modeling. *(E Al Nuaimi, 2015)* Therefore, all stake holders including public and private sectors and system developers are thereby compelled to accept the systems with constrained scalability and varying needs. However, because cyber threats appear to be well-managed, broad, and recognized, it is essential to raise awareness about smart-city cyber security and put in place appropriate measures to protect people's privacy and security. *(V Demertzi, 2023)*

According to the aforementioned, information/ cyber security is essential in intelligent cities to guarantee improved integrity, confidentiality and availability. Additionally, it guarantees the steadiness needed for national services and organizations to promote balanced living and smart environments.

Key Words: *Smart city, Cyber threats*, Interdependence, Cyber-attacks, Risk management

CHAPTER 1: INTRODUCTION

In the face of a changing cyber threat landscape, the scientific community must ensure threat, protection and response as smart cities will provide business with incomparable job opportunities. (Z Allam, 2022) However, the massive increase in the number of connected devices will allow cybercriminals to come to an unprecedented standstill. Smart city security should be a partnership between local governments and businesses that have a direct interest in the continuation of urban operations. (V Demertzi, 2023) In addition, to ensure the cyber security of the smart city, important features and security behaviors must be determined and monitored, thus forming the basis for the operation of the main support. (A Clim, 2022)
A city can be considered a smart city when investment in traditional infrastructure and human resources supports sustained economic development and good living action according to ICT. Smart cities can combine their productivity (which also doubles as natural resources) with communities, businesses and human resources to improve services and productivity, rehabilitation and long-term sustainability. (MGM Almihat, 2022) As mentioned before, the purpose of ICT is to provide intelligent management tools. The development of smart cities is happening all over the world. (M El Hendy, 2022) These arise from advances in information technology and open up new economic and social opportunities, while also leading us to more secure and personal prospects. (J van den Hoven, 2014) People are already connected with the help of devices such as smartphones. Smart devices, security and energy meters are used in many cities. The "Internet of Things" now connects entire buildings, cars, public places and other social networks. (AS Syed, 2021) The model is designed for all relevant systems. They will deliver unprecedented improvements in quality of life. To take advantage of these, new networked systems for monitoring, control and automation are being added to the city's infrastructure and programs. (P Bellini, 2022) Both public and private transportation are smart. Both the Internet of Things and Information and Technology (ICT) have many advantages. Smart home and healthcare devices, smart meters and security systems all provide unparalleled convenience and an enhanced lifestyle. (K Shahid, 2022) City infrastructure and services are constantly evolving with the introduction of new communication technologies for automation, monitoring and control. These will include providing clean water and toilets for first responders and emergency workers. (A Hangan, 2022). The legal, political and social security of the city should be as important as thought, management and business. (N Stern,

2015)

However, information security and smart management are closely related to each other. Risks and issues related to data security, including data transmission, processing, management, network security and access to devices, are significant. (Elvira Ismagilova, Laurie Hughes, Nripendra P. Rana & Yogesh K. Dwivedi, 2019) By reviewing and improving laws and regulations, strengthening business management, improving the level of protection, strengthening the sharing combination of new technologies, strengthening network access and strengthening self-identification security mechanisms, the aim is to strengthen law enforcement, protect the confidentiality of large amounts of data to manage and protect wisely. (S Kumar, 2019) Authentication needs to be more secure because there is only permission. Intelligent management services should be open to the outside world. To address the shortcomings of previous methods, this work presents three authentication technologies for government electronic systems. Authorization is achieved through a method known as hashing and lightweight XOR. (Farm, 2018)

1.1 Concept of Smart Cities

The term smart cities represents a paradigm shift in urban development, where technological innovation intertwines with urban planning to establish more efficient, suitable, and sustainable urban environments. At its core, a smart city leverages cutting-edge technologies such as IoT, AI and data analytics to gather vast amounts of information from various urban systems. This data-driven method enables smart city officials and planners to make prompt decisions, improve resource allocation and improve overall standard of life for residents.

Central to the concept is the idea of interconnectedness. By incorporating various aspects of urban life, from transportation to energy management to waste disposal and public safety, smart cities promote synergy among these systems, leading to smoother operations and improved services. For instance, real-time traffic monitoring and smart traffic lights can alleviate congestion, reducing commute times and environmental impact. Moreover, citizen engagement is bolstered through digital platforms that allow residents to voice concerns, access information, and actively participate in shaping their urban surroundings.

However, the concept of smart cities extends beyond technological prowess; it underscores a commitment to sustainability and inclusivity. As cities grapple with challenges like rapid urbanization and climate change, the adoption of energy-efficient buildings and roads, renewable energy sources and green transportation options becomes paramount. Equally important is the equitable distribution of smart technologies to ensure that benefits are accessible to all segments of the population. In this holistic vision, smart cities transcend mere technological showcases to become vibrant hubs where innovation and human welfare converge, shaping the urban landscape for generations to come.

The advancement of the smart city concept is a response to the increasingly complex and interconnected nature of urban life. Traditional urban models often struggled to manage the growing demands of urbanization, leading to issues like traffic congestion, pollution, inadequate infrastructure, and resource inefficiencies. By embracing technology and data-driven insights, smart cities intend to overcome these challenges and pave the way for a more resilient and adaptable urban future.

Crucial to the success of smart cities is the alliance between various stakeholders, including public agencies, private partners and citizens themselves. Open lines of communication and the sharing of ideas enable the co-creation of solutions that cater to unique urban contexts. As the smart city ecosystem continues to develop, it is essential for cities to prioritize data security and confidentiality to ensure that the benefits of technological advancement do not compromise the well-being of residents.

1.2 The Difference between “Traditional” and “Smart” Cities

Smart cities and traditional cities differ in various ways, primarily due to the incorporation of technology and data-driven approaches in smart cities. Here are some key differences between the two:

Technology Integration:

- **Smart Cities:** Technology is a central feature of smart cities. They extensively use sensors, data analytics, and IoT devices to examine and manage several urban systems, such as traffic management, waste management, energy management and public safety.
- **Traditional Cities:** While technology may be present in traditional cities, it is not as deeply integrated into the urban infrastructure. Basic technologies like traffic lights and public transportation systems are common, but they might lack the interconnectedness and data-driven insights found in smart cities.

Data Utilization:

- **Smart Cities:** Smart cities depends on real-time data collection and evaluates to make prompt decisions. This data helps to boost resource sharing, improve services, and improve urban planning.
- **Traditional Cities:** Data utilization in traditional cities might be more limited, often relying on manual or periodic data collection methods. Decision-making might be less data-driven and more based on historical patterns.

Efficiency and Sustainability:

- **Smart Cities:** Efficiency and sustainability are core principles of smart cities. These cities prioritize energy efficiency, resource optimization, and the reduction of carbon emissions through technology-driven solutions.
- **Traditional Cities:** While traditional cities may have sustainability initiatives, smart cities tend to have more advanced and integrated approaches to address environmental challenges.

Citizen Engagement:

- **Smart Cities:** Smart cities often emphasize citizen engagement through digital media and apps. People can contribute in decision-making, report issues, and access city services more conveniently.
- **Traditional Cities:** Citizen engagement in traditional cities might be more reliant on traditional methods, such as town hall meetings and physical service centers.

Infrastructure and Planning:

- **Smart Cities:** Smart cities incorporate technology into urban planning and infrastructure design, using data to optimize transportation systems, public spaces, and utility services.
- **Traditional Cities:** Traditional cities might rely on conventional urban planning methods, which could lead to less efficient resource allocation and infrastructure design.

Resilience and Adaptability:

- **Smart Cities:** Smart cities often focus on resilience and adaptability to rapidly changing urban challenges. Technological solutions can help these cities respond to crises more effectively.

- **Traditional Cities:** Traditional cities might face greater challenges in adapting to rapidly changing circumstances due to potentially less flexible systems.

Quality of Life:

- **Smart Cities:** The integration of technology can lead to enhanced quality of life in terms of reduced commute times, better access to services, enhanced safety, and increased convenience.
- **Traditional Cities:** Quality of life improvements might be present, but they could be less optimized compared to smart cities.

In summary, the primary distinction between smart and traditional cities lies in their level of technological integration, data-driven decision-making, efficiency, and the ability to adapt to changing urban demands. While traditional cities have their strengths, smart cities aim to address contemporary urban challenges with innovative solutions powered by technology and data.

1.3 Components of Smart Cities

Smart cities consists of several interconnected factors that work mutually to enhance urban living, sustainability, and efficiency through the use of technology and data. The specific components can vary depending on the city's priorities, but here are some common elements found in many smart city initiatives:

Information and Communication Technology (ICT) Infrastructure:

- High-speed internet connectivity and broadband networks serve as the backbone for smart city services, enabling data communication between devices and systems.

Internet of Things (IoT) Devices:

- Devices like radars, antennas, actuators and IoT devices collect and transmit data from various urban systems, such as traffic management, energy management, waste management, etc.

Data Management and Analytics:

- Data gathered from IoT devices is evaluated using sophisticated analytics tools to gain insights, detect trends, and make informed decisions.

Smart Transportation:

- Intelligent traffic management systems, real-time GPS navigation, smart parking solutions, and public transportation optimization are part of smart mobility initiatives to minimize road blocking and improve transportation possibilities.

Energy Management:

- Smart power houses, renewable energy sources and highly efficient energy systems are employed to monitor and control energy consumption which leads to reduced impact on environmental.

Waste Management:

- Smart solutions for waste collection such as smart bins that are equipped with sensitive sensors can improve waste collection methods based on fill levels, minimizing unnecessary trips and improving efficiency.

Public Safety and Security:

- Surveillance cameras, emergency response systems, and predictive policing algorithms enhance public safety and help manage security concerns more effectively.

Smart Governance and Citizen Engagement:

- Digital media, mobile applications, and other online websites/ services which facilitates public living in a smart city, allows people to give their valuable feedback and highlight their issues.

Environmental Monitoring:

- Sensors measure air and water quality, noise levels, and other environmental factors to ensure a healthier urban environment and prompt responses to pollution or other issues.

Smart Buildings and Infrastructure:

- Buildings equipped with smart technology can optimize energy use, lighting, and temperature control. Smart infrastructure includes roads, bridges, and utilities with embedded sensors for monitoring and maintenance.

Healthcare and Education:

- Telemedicine, digital health records, and smart education systems contribute to better healthcare access and educational opportunities for residents.

Economic Development:

- Smart city initiatives can invite huge businesses companies and entrepreneurs that focuses on technology and modernization.

Sustainability and Environmental Initiatives:

- Green spaces, eco-friendly building designs, water management systems, and initiatives to reduce carbon emissions contribute to a more sustainable urban environment.

Data Privacy and Security:

- Robust cybersecurity measures are essential to safeguard valueable data and guarantee the privacy of people living in a smart city.

These components, when integrated effectively, contribute to the overall vision of a smart city by enhancing quality of life, optimizing resource allocation, and improving the urban environment for residents and visitors alike.

1.4 Essential IT Services in Pakistan

The dynamics of a knowledge society and knowledge economy are shifting, and information technology is at the center of this transformation. Economic growth may be boosted using this factor. A Look into Pakistani News The information technology (IT) industry is gradually carving itself into a unique niche as a source of choice for outsourcing, BPO, and freelance software development. *(P Agarwal, 2019)* Freelance growth in Pakistan was rated #4 globally. Over the last three years, global IT exports have surged by 70%. Pakistan's digital economy is rapidly changing. IT/IteS.A major contributor to Pakistan's economic growth, the industry is proportional to almost 1% of Pakistan's GDP, or approximately $3.5 billion. The growth rate in the previous 4 years and prognosticators predict a further 100% expansion over the next budget of $7 billion in two to four years. At a whopping $1,067 million, IT exports just broke all previous records of billion in the 2017–18 fiscal year, up from $939 million the previous year preceding fiscal year. *(Dawn.com, 2022)*

According to Pakistan's Central Bank, the amount is $700 million (SBP). However, Freelancers in the nation provide an additional $1.2 billion to the country's exports. An amount that is not registered with the central bank. These businesses generate extra export revenue of $600 million that do not contribute financially to Pakistan.

Pakistan's government is committed to fostering the growth of the country's IT sector. In order to build a technology park in Islamabad, the country's ministry of technology and the Korean government recently struck a deal worth PKR 10bn. Innovation in technology In every country where development has taken place, SEZs have played a crucial role. *(dunyanews.com, 2021)*

The PM's Package includes Tech Special Zones, which will benefit businesses who are relocating to the area money put into Pakistan. The IT industry in Pakistan has doubled in size over the previous four years, reaching $3.5 billion, and analysts predict that this figure will increase by another 100% this year. The following two to four years. *(BR Web Desk, 2022)* Pakistan's information technology sector is teeming with skilled professionals who are absolutely able to fulfil market's demands at affordable prices. As the 3G and 4G services are introduced, internet penetration has skyrocketed. Since every year 10,000 IT startups are launched in Pakistan, the country has recently seen a growth in the number of incubation facilities and accelerators, resulting in a swarm of new grads. During Q1 of FY16, the mobile wallet (m-wallet) channel handled 21.8 million transactions with a total value of $3.07 billion.

Protection of personal data and online privacy for increased transparency and security of sensitive information via adequate Data Protection legislation; promulgation of required policy frameworks, regulations, and norms to allow construction of a sustainable IT ecosystem. *(Cannataci, Joseph A., Bo Zhao, Torres Vives, Gemma, 2016)* Construct a plan for the future of cloud computing and related services; data privacy, and transparency requirements, data ownership rules, and data categorization mechanisms are all examples of regulation security. The Ministry of Commerce and I will continue working together to create a framework and Policy for electronic commerce in e-commerce consultation with appropriate parties. These include enacting the right kind of rules and taxes simplifying, facilitating commerce, resolving disputes digitally, protecting consumers' personal information, etc. Encourage using digital signatures to authenticate further and protect sensitive data. Adjustments to e-Government-related regulations and statutes, including for use with e-workflows, e-approvals, and e-processes, such as "Rules of Business," "Secretariat Instructions," etc. *(J Sen, 2013)*

1.5 Threats and Attacks

A dynamic phenomenon and process, "the art of war" addresses when, when, and how to confront the opponent. The world faces a new peril that poses problems for nations and the private profit-driven world. Massive amounts of money are laundered or stolen, personal information is made public, state secrets are obtained, and vital public infrastructure is breached. Cybersecurity pertains to the Internet and its many connected devices. Cyber security concerns are growing in number and severity as the globe becomes increasingly interconnected and digitized via the Internet and other forms of information technology. *(ZM KHALILZAD, 1999)*

Furthermore, Pakistan is certainly not an exception. It is becoming more likely that a nuclear state in a strategically significant location will be the target of cyberattacks. Business and independent employment are further examples. Numerous people in Pakistan utilize the Internet, and the country's increasingly digitalized security apparatus and financial system rely on it. *(MR Shad, 2019)* Pakistan has also enacted regulations to deal with the danger posed by cyber-attacks, but they do not seem to be comprehensive enough to deal with the full scope of the problem. We need to constantly evaluate the state of the threat landscape and adjust our approach as appropriate to counteract the ever-evolving dangers posed by our many different enemies. *(UP Khan, 2020)* Based on this vantage point, the report evaluates Pakistan's cyber domain, identifies problems, and suggests solutions. In addition, it addresses the progress of the law in Pakistan and offers suggestions for the future. In 2021, there was a noticeable increase in the number of cyber assaults targeting small firms, and this trend is expected to continue in 2022. *(tribune.com, 2021)* If your company wasn't one of the almost halves that suffered a cyber assault this year, consider yourself fortunate. However, your good fortune will eventually run out, so if you have not given much attention to security in the past, now is an excellent opportunity to receive the type of cybersecurity education that may help secure your company.

Smart cities are becoming increasingly prevalent worldwide as city planners and administrations look to improve the efficiency of urban living. A key element of smart city development and planning is the introduction of a concrete cyber security policy to protect the data and infrastructure of the city from attack. *(E Ismagilova, 2020)*

Pakistan is no stranger to the threat of cyber attacks, with a number of high-profile incidents in recent years. In 2016, Pakistan was hit by the ‘Karachi Cyber Attack’ which saw hackers stealing sensitive data from Karachi’s water utility company. This was followed by the ‘Peshawar Electric Supply Company Cyber Attack’ in which hackers again made off with confidential data.

Given the increasing importance of smart cities, it is essential that Pakistan develops an effective cyber security strategy to protect its urban centres from attack. One way to do this is through risk management, which involves identifying, assessing and prioritising risks. By taking a risk management approach to cyber security, Pakistan can develop a proactive and comprehensive strategy for protecting its smart cities from current and future threats. *(SY Yoon, 2020)*

1.6 Significance of the Research

Research on risk assessment of a smart citiy is of paramount significance as it provides a structured and comprehensive understanding of potential vulnerabilities and threats that arise from the integration of advanced technologies into urban environments. By identifying and analyzing these risks, cities can proactively develop strategies to mitigate negative impacts, thereby safeguarding critical infrastructure, data integrity, and citizen privacy. Such research ensures that the benefits of smart city innovations are maximized while minimizing potential pitfalls, leading to a more secure and resilient urban landscape.

Moreover, the outcomes of risk assessment research inform evidence-based decision-making for urban planning, policy formulation, and resource allocation. By quantifying and qualifying potential risks associated with various smart city components, city officials and policymakers can prioritize investments and allocate resources effectively. This approach optimizes the allocation of funding, time, and efforts toward strengthening security measures, building redundancy into critical systems, and implementing robust data protection protocols. The result is a city that not only embraces technological advancement but does so in a manner that aligns with the best interests of its residents and stakeholders.

Furthermore, research on risk assessment fosters, partnership with various stakeholders, including public sectors, technology providers, researchers, and citizens. This collaborative approach promotes a holistic understanding of the challenges that smart cities may face and encourages the development of interdisciplinary solutions. As cities strive to build trust and transparency with their citizens, research-driven risk assessment becomes a means to effectively communicate the proactive measures being taken to address potential risks. Ultimately, the significance of research in this domain lies in its ability to empower cities to navigate the complexities of the digital era while prioritizing safety, sustainability, and the well-being of their inhabitants

CHAPTER 2: CYBER THREATS

Since it is difficult to pin down who is responsible for a cyber attack, both politically and technically, hostile actors may often get away with their actions without being held accountable, leading to a "dominantly offensive" climate. Government infrastructure and security systems have the same technological vulnerabilities as the commercial sector since they use shared supply chains and rely on the same handful of ICT platforms. *(Myriam Dunn Cavelty, Andreas Wenger, 2022)* Due to outmoded global governance, bad actors may now cause mischief while remaining just below the line that would prompt a reaction. As a whole, these issues pose a threat to international peace and security, and countries and international organizations are scrambling to respond. *(W Durch, 2016)*

The massive consequences of a cyberattack are again brought home by the October 29 cyberattack on the National Bank of Pakistan. The world of cyberspace is one that humans have created. It is all around you and helps you accomplish things like work and survive in the wild. Innovations in cyberspace sparked an information revolution, which morphed into the fourth industrial revolution (4IR) thanks to the widespread implementation of latest technologies like AI, IoTs, machine learning and extensive data (big data). *(Salam Siddique, 2021)*

State and non-state actors may boost their benefits and further enhance their agendas thanks to the Internet. While cybercriminals attack for financial gain, nations increasingly exploit the Internet as a new realm to project influence. Cyberweapons with military capabilities are being used for political ends. (*M Eilstrup-Sangiovanni, 2018)* The Stuxnet infection demonstrated that advanced software may now be used to destroy a physical target, adding a new dimension to cyber warfare. Another example of the intricacy of cyber weaponry is the Pegasus malware, which allows a predator's call, whether it is answered or not, to hack a prey's mobile device and take private information. *(Yuri Diogenes, Erdal Ozkaya, 2019)*

Even though Pakistan is a developing nation, it has a very respectable internet penetration rate: 77.7 percent of the population has a mobile subscription. The Government of Pakistan announced the Digital Pakistan project in 2018 to improve the country's infrastructure in the digital sphere and inspire a new wave of creativity and entrepreneurship. Earlier administrations have helped facilitate the IT industry by lowering tariffs. The PM Laptop Scheme and similar programs significantly raised computer literacy rates. Digital transformation includes the implementation of several information technology solutions. These include the NADRA database system, the land computerization record system and the online tax return system. IT solutions like edTech and FinTech flourished during the Covid-19 outbreak and played an essential role in keeping people alive. During this time, there was also a substantial increase in the volume of online. (moib.gov.pk, 2018)

2.1 Cyber Threat Policy

The previous decade has seen the globe transform into a true Global Village thanks mainly to the advancements in ICTs. A new development in ICT is altering how we think about global economic growth, creating new avenues for users in commercial, economic, cultural, and social spheres about the Internet and computer networks. *(Shing H. Doong, Shu-Chun Ho, 2012)* The new age that this explosive expansion has brought in is one of extraordinary convenience. As well as ubiquitous low-cost access to globally linked networks. Thanks to the development of modern means of communication and dependence on Broadband infrastructure in particular, the Internet has become the focal point of the contemporary era. As the world is nowadays, individuals have more access than ever before to global information networks, data, know-how, and understanding. *(J Naughton, 2016)* The growing number of occurrences involving malevolent ICT usage in cyberspace threatens state guarantees of civil liberties, an even playing field, transparency, and social and economic stability, putting all kinds of people in danger, including their money and personal safety Effects on people, organizations, industries, and governments at the local, national, and international levels might be devastating difficulties in overcoming obstacles to progress in many economic areas. *(I Dobák, 2021)* Set up a system of checks and balances for a safe online environment in order to protect our nation's critical infrastructure from cyberattacks and infrastructure. Protecting sensitive data and facilitating communication across organizational levels are two primary goals. First, the ability to keep an eye out for dangers, identify them, defend themselves, and second, counterattack a country's network of computers, the Internet, and other electronic devices. The goals of this mandate are:

- To safeguard the nation's critical information infrastructure guidelines for national security in the design process, The process of acquiring, creating, deploying, and operating an information system.

- Establish a system of checks and balances for the safety of sensitive data via audits; governmental and private organizations must adhere to the same standards. Protect the honesty of information and communication technology by creating a system of diagnostics, screening, investigation, and accreditation.
- To ensure people's privacy when using the Internet by providing the necessary help and infrastructure for any interested agencies. The public and private sectors may form productive alliances and cooperative structures through shared efforts in technology and operations.
- Raise awareness about cyber security nationwide by informing and enlightening the general public. Through capacity development, we aim to:
- Train highly competent Cyber Security experts; Programs for the enhancement of Knowledge and Training Skills. The goal is "to promote and sustain indigenization and growth of Cyber Safety measures developed by joint private and governmental research and development initiatives.
- To lay forth a plan for intergovernmental collaboration on a global scale and partnerships in the field of cyber security. Legislative and regulatory activities must be identified and processed to meet the responsibilities outlined for various parties involved in the policymaking process. The Cyber Security risks must be regularly controlled. Prompt the use of a risk-based Cyber Security strategy, frameworks for regulation, assurance, threat analysis & Incident Management.

2.2 Cyber Protection Policy

To safeguard government digital services, creating an IP reputation service is necessary. (It would be possible for digital services to acquire data about the IP address of a user connecting to the service to improve your knowledge for making timely choices on risk management. To make sure that government networks are secure, you should:

- Try to have your goods installed; there is operating normally and are not being tampered with maliciously.
- Explore options for growing your digital service offerings outside the gov. pk domain. Protect the nation's critical information infrastructure, ICT, Next Generation(s) mobile service and networks, and related assets via the maintenance of the necessary

technological platforms, security for the IoT, and the part of Government in shaping economic development in the nation. *(exabeam, 2021)*

- Promote "accountability" and "self-governance" norms by highlighting the benefits they may bring to society that government and business entities will each be held accountable for protecting their digital property, information, and offerings in order to enhance in terms of privacy, reliability, and accessibility actions that alert people who are using obsolete software or hardware. The exchange of private and public sector secrets companies, protecting people's right to privacy while using the Internet, and ensuring security for every piece of information. *(EPRS, 2019)*
- Get systems set up to locate Critical Information Assets, rank them in importance, evaluate their security, and safeguard them from harm; utilize cutting-edge safety procedures to guarantee a safe ICT setting, including mobile devices and cloud-based solutions. Insist that all important institutions in the country must adhere to national security companies in the area to lessen the possibility of disruption. Build a system to safeguard essential files. Organizational infrastructure and its incorporation through appropriate. The need to set up and enact strict Cyber Security risk management procedures, among other things, in accordance with any of the relevant international standards. *(Y Sun, 2014)*
- Organization (ISO)/International Information Systems Auditing and Control Association (ISACA) RISK IT, etc., Strive toward safeguarding the associated digital infrastructure and service.
- Stakeholders will have access to all government systems with the required and desired functionality to meet a particular requirement in the public sector's information infrastructure. Technology for restricting access Promote the development of co-located national Data Centers technology for telecommunications and server hosting to ensure that all government agencies have access to high-quality infrastructure, state and national, or state and provincial. *(moitt.gov.pk, 2022)*
- Clearly define and implement a strict Government Authentication and Data Framework for Data Protection, Classifying Data and Making Sure data security measures are in place. To manage risks and implement patches, you must use each and every one of the Government's technological infrastructures. *(techtarget, 2022)*

- Collaborate with appropriate government bodies to make allocation obligatory, allocation of funds from the ICT project budget for Cyber Securite. Make a plan for how the Screen and approve national security standards to implement the "Cyber Security by Design" notion in ICT goods and services.
- Develop and deploy state-of-the-art cyber forensics and screening infrastructures to protect against sophisticated cyberattacks in a world dominated by AI technology.
- Develop a methodology for ensuring data accuracy in cyber security audits. Both public and private organizations sectors must follow the regulations. You need to set the infrastructure and use what is already there to your advantage—resources for determining conformance and proving it, Recommended procedures, policies, and recommendations for cyber security.
- Validation against PCI/PA DSS for financial institutions, the Information Security Management System (ISMS) standard, or any of several different norms and regulations comparisons, audits of the internal security, and tests for vulnerabilities in the system.Foster an atmosphere conducive to entrepreneurship via collaborative efforts on the part of the Government, private sector, the academic community, and research institutes in various fields, such as supply chain risk management, etc. *(IC Wilkinson, 2020)*
- The Government should assist newly established businesses and make it easier for them to expand into competitive firms.
- Give privately held cyber security companies and organizations the ability to participate in work in conjunction with governmental agencies and control the activities of such bodies.

Act as a conduit for disseminating information about creating new legal and regulatory frameworks between relevant parties. Any alternative framework that the Federal Government determines to be suitable.

2.3 Implementation of Cyber Threat Policy

The lack of a comprehensive policy and plan for cyber security makes it more likely that measures to secure the Government's digital assets would be haphazard and uncoordinated.

- Pakistan's digital assets need to be adequately protected by the country's current Cyber Security laws. The current Cyber Security laws need to go further in providing a practical framework and have to be drastically altered if it continues to hold people's attention to the letter and the spirit of the law of the land. Furthermore, a suitable and appropriate legal framework may facilitate conformity with a centralized and powerful regulation structure. *(pakobserver, 2023)*

- Cybersecurity's legislative framework, institutions, and procedures must be monitored and assessed at all times and improvement of same should also be underscored or else they will lose efficacy and fall in danger. Specifically, the Cyber Security Framework and its Constant implementation vigilance, analysis, and policy refinement are required. Moreover, using relevant legal and technological framework structures might aid in identifying risks and repercussions connected so that it could adequately probe, and there would be no exposed weak spots to be used as a tool by bad people. *(H Taherdoost, 2022)*
- Weaknesses in Cyber Security will result from an inability to keep up with the ever-expanding area of Cyber Security, which requires a constantly updated set of relevant skills and resources. In addition, a supply-demand gap may be bridged; a growing problem is the skillset gap in the digital workforce. Negative connotations are attached to the lack of technique for guaranteeing a sufficient supply of high-quality human and material resources is a countrywide cyber security risk. *(C Feijao, 2021)*
- With little to no bilateral agreement among parties, countries risk having their data "colonized" or handled, controlled, and processed outside of the country's legal authority. The information space is vulnerable to contamination by threat actors, and citizen data may be sold to unapproved parties without authorization or approval—this kind of multiplication. Because the misuse of information leads to the exploitation of some groups within society, the data quality, quantity, and management are all subpar, and there is a lack of data, to begin with; governance threatens the reliability of data by producing resources that are prone to error.

2.4 Pros and Cons of Cyber Threat Policies

PROS

- Use firewall software to cut down on the number of malicious attempts to reach your system and make cyber security the most effective instrument for increasing the efficiency of your data and its network. *(John M. Borky, Thomas H. Bradley, 2018)*

- Cybersecurity makes a significant dent in the likelihood of a data breach occurring. Restricting access to resources based on user capabilities and duties or network connections may be accomplished by using DLP strategies in combination with a web server, firewalls, and several other methods and tools for access control.
- Integrated security measures are required to comply with some legislation. It is possible to manage a global business while also managing confidential information about one's customers, such as their social security numbers or credit card details. The European legislation on data privacy may apply to your system. The use of appropriate protections is required in order to prevent unauthorized access to or theft of such information. *(Network world, Vol. 8, No. 26)*
- Terrorist organizations and other enemies may be able to steal or even leak vital government information because cyber security measures are lacking. The immediate and severe economic and political implications that will befall nations that fail to handle this problem will be harsh. *(OA Hathaway, 2012)*

CONS

- Cybersecurity systems are impractically expensive to set up and maintain individually. Integrating hardware and software and hiring staff with cybersecurity expertise are both crucial.
- A cyberattack or other assault might significantly damage your business, but the expense of preventing damage could be far higher.

- You may be spending money if the proper personnel are not in place to finish the implementation. Furthermore, since the threats constantly evolve, you will need to follow any new cybersecurity requirements. Lastly, a company's size or financial situation may prevent it from employing a dedicated IT department. *(H de Bruijn, 2017)*
- The company's overall production would suffer due to the deployment of cyber security measures. For instance, to set practical constraints, businesses may mandate that workers use complicated credentials for each session or two-factor authentication whenever they access a system from the comfort of their homes. *(D Bourgeois, 2014)*

CHAPTER 3: LITERATURE REVIEW

One division of ICTs is the smart city. Applications for it include home appliances, transportation, and environmental protection: health care systems, security development systems, and numerous others. *(AS Syed, 2021)* IoTs are frequently used in practical situations to make these applications work. One of the keys to implementing smart cities is data security. *(T Alam, 2021)* Challenges and to address these security concerns, numerous Techniques for protection have been suggested. As a result, they provide technological solutions for creating smart cities. *(MHP Rizi, 2022)* Several continents come from various geographic areas, including Asians, Americans, and the goal of smart mobility is to "smarten up" transportation systems. By enhancing accessibility for local and international travel, The public may benefit significantly from smart transportation networks. Consumers can use mobile applications focused on transportation to set their schedules and identify the most optimized route. *(TW Lim, 2019)* This is made possible by ICT from contemporary and balanced smart transportation. Applications for smart mobility facilities commonly include Passports for drivers and license readers, automobiles looking for a parking spot, and forecasting. Europeans put the idea into practice to control their cities, smart cities.

Traffic safety is an important and highlighted issue in urban cities that endangers people's lives. Also, IoT may take the initiative in recognizing *The Prevention of Human Errors and Their Limiting* road accidents. For instance, a specific study provides insightful information about enabling smart mobility systems in the literature. *(AS Syed, 2021)* An IoT-based concept was developed by merging internet and affordable aerial technologies. The proposed study indicates the potential of tracking traffic safety utilizing IoT advancements. It provides a low-cost IoT platform for evaluating a road network's safety. *(K Lawal, 2021)*

Additionally provides a summary of the important IoT technologies recommended for efficient movement in scenarios involving smart cities. IoT technology is essential for developing intelligent transportation systems. However, IoT devices cannot guarantee the security they offer. The instrument frequently has low processing speeds, and its hardware limitations preclude them from having internal security features. *(P Bellini, 2022)* The gadgets become vulnerable as a result. Strict security guarantees are required for the IoT instrument that controls a smart city's vital transport infrastructure. Vanet provides the infrastructure necessary for moving vehicles to communicate with one another and share information on accidents, traffic jams, and other road conditions. Vanet is a superb cyber-physical system, but it has a number of security and privacy issues, notably with regard to location privacy. They must improve the Vanets applications before they may be used to protect the privacy of cars' identities and locations. However, since it is not possible to use the privacy protection strategy to monitor traffic conflicts in the case of network security, most users would like to have a self-defense method to prevent installation in certain situations. In order to offer conditional privacy preservation, group signatures may be employed. *(N Ahmed, 2022)*

According to what was previously stated, Connecting and strengthening human networks is what ICT is all about, so it seems sensible that the technology exists to do just that. Organizations and generally accessible resources in order to promote long-term economic growth, high standards of living, and general well-being for the lion's share of the population. *(A Joshi, 2013)* That is why we need a solution like concept of smart cities. This concept uses ICTs to address public issues but does so through the management of natural resources via a collaborative effort including a wide range of interested parties disasters as the top priority, through citizen participation and participatory action and preventing risks. Therefore, smart cities ensure a connected urban community that reaps the advantages of savvy administration. n while incurring the fewest possible economic, administrative, and social expenses. *(R Sánchez-Corcuera, 2019)*

3.1 Dimensions of a smart city

Four pillars are necessary for the construction of smart cities: physical, institutional, economic and social infrastructure. Various dimensions of the smart cities are designed using these pillars. These dimensions are discussed in this section, focusing on their definition, dominant used technology and smart applications

A smart city is generally planned according to four pillars: infrastructure, physical development, social and economic development. Smart cities are measured to support these pillars. This section discusses aspects of smart cities included in the literature, including definitions, smart applications and technologies (Figure 3.1).

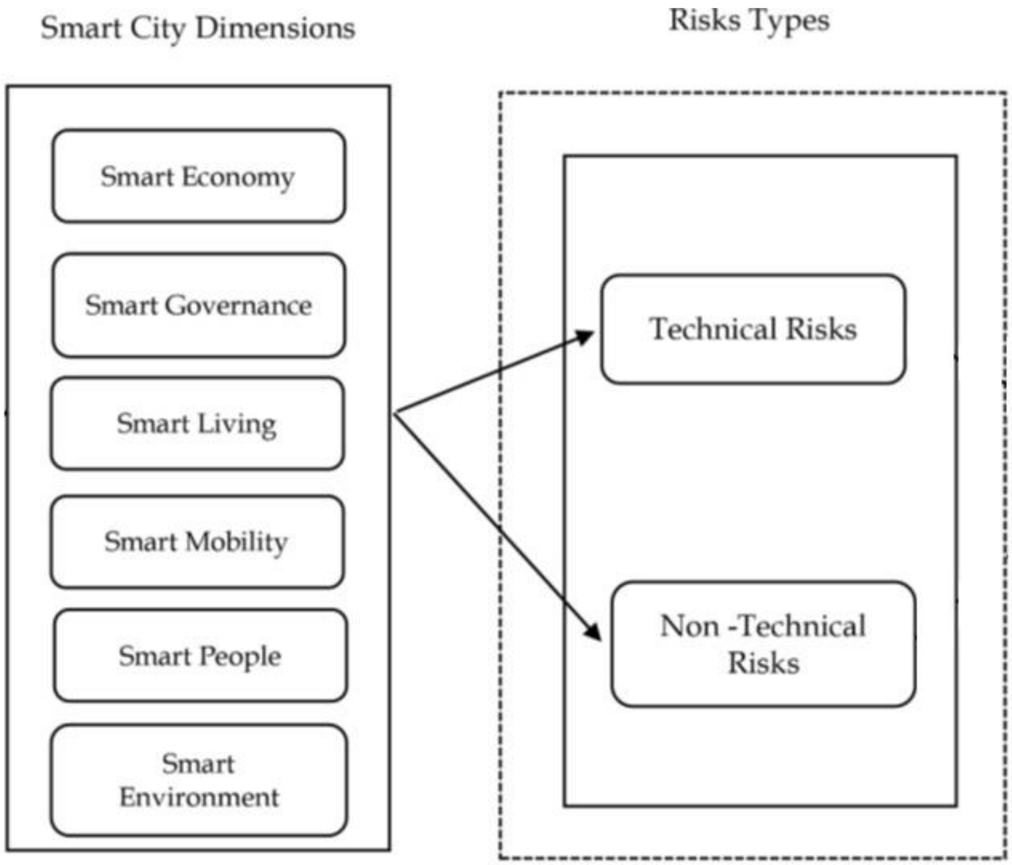


Figure 3.1 Dimensions of a Smart City

3.1.1 Smart economy

Smart business includes guidelines and policies that encourage innovation and creativity, as well as attention to scientific research, technology and the concept of environmental sustainability. Kumar and Dahiya (2017) Business intelligence means business or knowledge. Business as any discipline; business, commerce, heritage, architecture, planning and development, management etc. It comes in many forms, each with its own unique features, challenges, and solutions.

Define business acumen as business knowledge based on the status quo. - Cutting-edge research across all disciplines including science, business, economics, heritage, architecture, planning and development. Smart work in smart cities comes in many forms and applications; each has unique features, challenges and solutions

.

3.1.2 Smart governance

Silva et al. (2018) examined the dimensions, challenges, and solutions of smart cities. The author recommends smart city management and decision-making, healthcare, transparent management, and shutting down public services. policy and strategy. The author believes that governance is a partnership between leaders and citizens. Only good governance can deliver maximum results regarding efficiency and trust in public, private and public administration. Ismagilova et al. (2019) highlight the benefits of using cloud-based services due to their benefits in decision making through collaboration, collaborative support, and information sharing.

3.1.3 Smart living

Ismagilova et al. (2019) consider smart lifestyle as another important aspect of the smart city. Apostol et al. (2015), smart business has a direct impact on smart life. According to the literature review by Romero, Gu'edria, Panetto and Barafort (2020), the use of ICT improves the quality of life through the use of electricity generated by the communication and network in the home, air conditioning and security connections. The author also said that smart homes are operated by applications related to smart services, such as collecting the owner's personal information without affecting their privacy and security.

3.1.4 Smart mobility

According to Appio, Lima, and Paroutis (2019), smart travel is related to the city's transportation system and systems. In smart mobility systems, information about traffic, congestion, travel time and delays is collected to provide solutions to traffic management problems. The use of intelligent communication will help people choose collaboration by sharing their information in real time (Silva et al., 2018). Ismagilova et al. (2019) To ensure safety and efficiency, in-vehicle data connectivity through the Internet of Things and Internet of Vehicles (IoV) plays an important role in smart transportation.

3.1.5 Smart people

Human capital and financial capital together form the infrastructure of smart cities. While human capital refers to the capabilities of an individual or group, social capital refers to the quality and quantity of relationships. Smart life can achieve productivity and innovation with better investments. Higher education such as schools, colleges and universities also play an important role in building human resources. These universities encourage people to become wise by acting as mediators, healers, and protectors. (Ismagilova et al., 2019). Artificial intelligence and big data, two major technologies, are required to create smart applications that enhance learning, knowledge sharing, and teaching (Radu, 2020). However, using these services may compromise security and privacy.

3.1.6 Smart environment

Smart environment is a system that helps manage waste, manage energy, develop smart projects, buildings and spaces, as well as control pollution and improve air, water and green spaces. Pollutant emissions are also controlled by smart environmental systems. Staff and Horelli (2014) talk about the use of technology to sustainably protect natural resources. Technology helps with this by creating applications related to smart spaces. This technology uses different types of sensors to control the smart space. Decision makers use real-time information from these applications to manage waste; through disposal, recycling or distribution.

3.2 Risks in a Smart City

In smart cities, every aspects of life is automated like transportation, economy, logistics, education, healthcare, maintenance and what not. Every aspect of human life is controlled by computerized technologies which requires human input and their finances. Hence, the smart cities also imposes risks. These risks are commonly categorized into two categories including technical risks and non-technical risks.

3.2.1 Technical risks

As the name suggests, such risks depend on technology and usage, and risks related to the Internet of Things, big data and intelligence are also important panics. Technology risks fall into three broad categories: technology selection, urban planning services, and technology implementation. Ahad et al. (2020) risks; He stated that it includes risks such as network security, connection between devices and systems, lack of infrastructure support, chaotic information management, compliance with different standards in technology and integration.

3.2.2 Non-technical risks

Non-technological risks differ from business risks in that these risks have nothing to do with technology. Although non-technical risks have a significant impact on smart city implementation and performance, they are often ignored by stakeholders. Risks arise from poor governance or weak public-private partnerships.

3.3 Smart Mobility

Smart mobility is responsible for the creation of better transportation system through the management of physical and IT infrastructure. It is an intelligent mobility network which supports better transport system. It connects various elements of technology such as tradition transport system (buses, cars, motor vehicles, trains), On demand ride sharing (Careem , Yango), Transportation system for delivery of assets (postex, drones) In short Smart mobility is fast growing ecosystem of Physical and digital resources:

Physical Elements: Physical Elements include all types of personal, shared and commercial automobiles, their data exchange capabilities and connection of road infrastructure i.e. smart traffic lights, CCTV cameras, toll gates, road sensors, etc

Digital elements: This includes all the applications which are Cloud-based and support the connectivity and management of physical assets including applications, software and traffic management systems.

3.3.1 Advantages

The advantages of smart mobility may include:

- Road Safety
- Revenue Generation
- Less Traffic Congestions
- Efficiency (better time management)
- Real-time data sharing
- Decreased CO2 emissions

3.3.2 Disadvantages

The disadvantages of smart cities related to transport and mobility includes:

- Public Private partnership
- Building infrastructure
- Security and safety
- Environmental pollution
- Cyber attacks on digital transport networks

The construction of proper roads and parking can build better public-private partnerships. The efficiency of road safety and urban mobility can significantly increase by integrating smart solutions to infrastructure, public transport system and traffic data Moreover increasing the urban economic growth and sustaining businesses. The connectivity of Vehicle and infrastructure by using various radars, antennas and CCTV technologies would transfer real time information to drivers and customers to help them avoid dangerous activity. Additionally, pollution can be minimized by usage of electric and environmental friendly motor vehicles. Lastly and more importantly, by Adopting best Cyber security measures, regularly updating your devices and analyzing third and fourth party risks can decrease the risks of cyber attacks on digital transport networks.

3.4 Research Gap and Research Question Formulation

In order to classify the risks associated with a smart city following research questions are formulated:

RQ1: What are the various risks associated with smart mobility? and which are dominant among them?

RQ2: What steps can be taken to mitigate these risks?

CHAPTER 4: PROPOSED METHODOLOGY

4.1 Proposed Framework

From a sustainability and security perspective, the types of risks associated with smart cities are different. Conditions, time and environment also vary in their impact on the risks posed by smart cities. The risk management model aims to prevent risks in advance according to the type of risk and reduce the impact of risks when they occur (Figure 3.1). This model divides the risks of smart cities into controllable and uncontrollable risks, as well as external risks and internal risks that focus on where they occur.

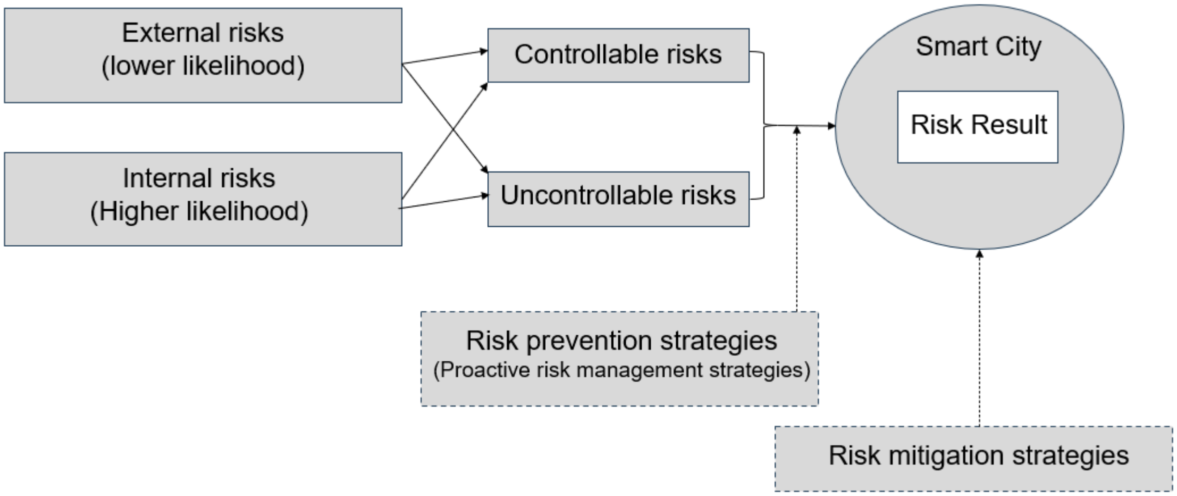


Figure 4.1 Framework/ Smart City Risk Management Model

Remember that many of the risks that arise cannot be controlled, but their effects can be reduced. Therefore, managers need to calculate the magnitude of each risk so that they can react accordingly. For this purpose, the concept of risk management (RMA) was introduced by Souza et al. Gray's method can be used to resolve the uncertainty of risk information. With partial knowledge of information, gray theory can be used to solve problems of uncertainty or risk. This method uses Gray numbers on known and unknown data. The Gray number is represented by the Gray number boundary between the known and the unknown.

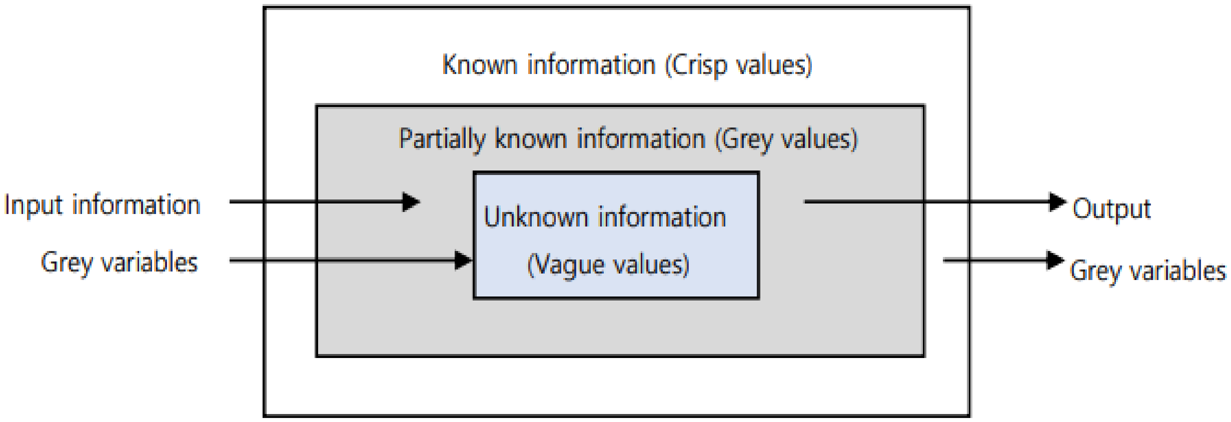


Figure 4.2 Grey Theory Concept

Britto et al. [27] used the Gray-based ELECTRE method for risk classification. Li et al. [26] used the gray decision method as a supplier selection problem. Memon et al. [28] combined gray system theory with fuzzy logic and applied it to the supplier selection problem. Baskaran et al. [29] used Gray's method to evaluate the stability of textile materials.

4.2 Risk Mitigation Strategy

Souza et al., [10] use value-at-risk (CVaR) to measure the risk associated with the supply chain and calculate the risk as probability of occurrence × consequence) which affects the risk assessment of the supply chain. . In response to the risk, this research has developed a risk management plan for impact and probability as shown in the table below. 4.1 and allocate costs according to the magnitude of the risk. In Table 4.1, the impact is classified as low, medium or high; The probability (frequency) is classified as low, medium or high.

Impact on Smart City	Risk Management Action		
High	Extensive level of management is required	Risk must be managed and monitored	Extraordinary management is required necessarily
Medium	Level of risk may be acceptable with monitoring	Meaningful effort by management is required	Low level Management effort is required
Low	Risk needs to be documented only	Risk needs to be documented along with monitoring	Risk may be monitored or managed as required
	Low	Medium	High
	Probability		

Table 4.1 Risk Management Actions

In the Table. 4.1 Risk management is divided into nine areas based on probability and impact. Each region is represented by a number. If a risk occurs in the smart city, the value of the risk is provided by risk management. However, the distribution of impacts and results is defined as low, medium and high. It is difficult to analyze the impact of smart city risk at all levels due to simple classification. Additionally, the issues that arise are framed as a score, with no insufficient objectivity or rationality behind each score. Therefore, in addition to classifying impact and probability and scoring risk management, appropriate objectives and appropriate procedures need to be carried out.

When problems arise in the smart city, various methods are used to prioritize risks through reliability and efficiency, risk assessment. Interventions and risk factors are used in this study. If the impact and probability classification of the risk encountered is too simple, it will not give specific results of the risks encountered. On the other hand, if the distribution of the impact and the probability are very different, the connection between the possible risk will not be affected. Explain that each risk is independent and can be separated effectively. Therefore, the classification of relevant risks and their probability of occurrence is included in the general process of creating the appropriate classification by collecting the information and opinions of experts who understand smart cities. In other words, quality attributes include not only algorithms and tools but also metrics to incorporate expert knowledge into research. It can provide better results. Therefore, this study used the gray method described in Section 4.1 to present the key management results in Table 4.1 through a clear and objective process. This study uses the gray process and risk management to implement risk mitigation strategies and then translate quality points into objective and reliable quantitative measurements.

CHAPTER 5: CONCLUSION AND FUTURE WORK

5.1 Conclusion

The concept of smart cities emerged as a response to the goal of building the city of the future, which is intended to be a place where the resident's and industry's well-being, as well as their place where people's rights are upheld and where the quality of city planning is assessed from the perspective of ecological and long-term viability, practices. The implementation of comprehensive cyber and privacy ICT solutions is an unavoidable prerequisite for the development of intelligence. These solutions must guarantee that the numerous components that go into constructing the city's structure can communicate. They should also reduce the possibility that several technologies will become outdated. Because of the wide range of infrastructures and the high level of activity in their working environments, there has to be a constant simplification of a process, expansion works are processed more quickly, and new features are included that are equal. It is necessary to fulfill these standards. As a bonus, unified management provides distinct and unambiguous approaches to providing end-to-end smart services predicated on rock-solid security needs and protecting the confidentiality of transmitted information to provide excellent services.

This study presents a smart city risk management model to detect various risks emerging in smart cities, respond effectively to them, enhance the strength of smart cities, and increase stability. Thanks to information and communication technology, smart cities can be confined to virtual cyberspace. However, since it is a physical place where people live and where many activities such as work are carried out, it is impractical and undesirable to conduct research in a single area. Risks associated with the smart city must be eliminated before they occur and therefore have no impact on the smart city. This study defines risk prevention strategies as creating effective protection policies before risks arise. If a risk occurs despite protective policies for prevention, the impact of the incident must be minimized for the smart city to be strong and stable. However, this study offers a smart city risk management model that can cope with various risks that arise in smart cities.

5.2 Future Work

In future, quantitative evaluation factors will be presented to evaluate the risks management model of a smart city and verify further the authenticity of this model after implementation and acquiring results. Many activities will be planned according to risk management based on the classification of risks.

REFERENCES

1. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber security challenges of deploying IoT in smart cities for healthcare applications. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 140–145.

2. Ganguly, P.; Nasipuri, M.; Dutta, S. Challenges of the existing security measures deployed in the smart grid framework. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 1–5

3. Bai, Y.; Hu, Q.; Seo, S.-H.; Kang, K.; Lee, J.J. Public Participation Consortium Blockchain for Smart City Governance. *IEEE Internet Things J.* **2021**, *9*, 2094–2108. [

4. Cho, Y.; Oh, J.; Kwon, D.; Son, S.; Yu, S.; Park, Y.; Park, Y. A Secure Three-Factor Authentication Protocol for E-Governance System Based on Multiserver Environments. *IEEE Access* **2022**, *10*, 74351–74365

5. aved, A.; Kubler, S.; Malhi, A.; Nurminen, A.; Robert, J.; Framling, K. bIoTope: Building an IoT Open Innovation Ecosystem for Smart Cities. *IEEE Access* **2020**, *8*, 224318–224342.

6. Guo, G.; Zhu, Y.; Yu, R.; Chu, W.C.-C.; Ma, D. A Privacy-Preserving Framework With Self-Governance and Permission Delegation in Online Social Networks. *IEEE Access* **2020**, *8*, 157116–157129.

7. Mahrez, Z.; Sabir, E.; Badidi, E.; Saad, W.; Sadik, M. Smart Urban Mobility: When Mobility Systems Meet Smart Data. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6222–6239

8. Dong, C.; Wang, H.; Ni, D.; Liu, Y.; Chen, Q. Impact Evaluation of Cyber-Attacks on Traffic Flow of Connected and Automated Vehicles. *IEEE Access* **2020**, *8*,

9.Patel, S.T.; Mistry, N.H. A review: Sybil attack detection techniques in WSN. In Proceedings of the 2017 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 2Murino, G.; Armando, A.; Tacchella, A. Resilience of Cyber-Physical Systems: An Experimental Appraisal of Quantitative Measures. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 20194–25 February 2017; pp. 184–188.24–86835.

10. Lu, X.; Jing, J.; Wu, Y. False data injection attack location detection based on classification method in smart grid. In Proceedings of the 2020 2nd International Conference on Artificial Intelligence and AdvancKarimi, K.; Krit, S. Smart home-smartphone systems.

11.Threats, security requirements and open research challenges. In Proceedings of the 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), Agadir, Morocco, 22–24 July 2019; pp. 1–5ed Manufacture (AIAM), Manchester, UK, 15–18 October 2020; pp. 133–136

12. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access* **2020**, *8*, 118433–11847

13. Qiu, J.; Liang, X.; Shetty, S.; Bowden, D. Towards secure and smart healthcare in smart cities using blockchain. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; pp. 1–4

14. Poonguzhali, N.; Gayathri, S.; Deebika, A.; Suriapriya, R. A framework for electronic health record using blockchain technology. In Proceedings of the 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 3–4 July 2020; pp. 1–5.

15. Madyatmadja, E.D.; Abdurachman, E.; Gaol, F.L.; Pudjianto, B.W.; Hapsara, M. Potential impact of social media to support government services in jakarta smart city. In Proceedings of the 2018 International Conference on Information Management and Technology (ICIMTech), Jakarta, Indonesia, 3–5 September 2018; pp. 534–538

16. Ramachandran, G.S.; Radhakrishnan, R.; Krishnamachari, B. Towards a decentralized data marketplace for smart cities. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; p. 1–8

17. Bululukova, D.; Tabakovic, M.; Wahl, H. Smart cities education as mobility, energy & ICT hub. In Proceedings of the 2016 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), Rome, Italy, 23–25 April 2016; pp. 1–8.

18. Demertzis, K.; Kikiras, P.; Tziritas, N.; Sanchez, S.L.; Iliadis, L. The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. *Big Data Cogn. Comput.***2018**, *2*, 35.

19. Razzaq, A.; Hur, A.; Ahmad, H.F.; Masood, M. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), Mexico City, Mexico, 6–8 March 2013; pp. 1–6

20. Choong, P.; Hutton, E.; Richardson, P.; Rinaldo, V. Assessing the cost of security breach: A marketer's perspective. In *Allied Academies International Conference, Academy of Marketing Studies. Proceedings*; Jordan Whitney Enterprises, Inc.: Arden, NC, USA, 2016; Volume 21, p. 1

21. Levy, M.J.; Bissell, R. Overview of Critical Infrastructure. In *Preparedness and Response for Catastrophic Disasters*; Taylor & Francis Group: Boca Raton, FL, USA, 2013; p. 151.

22. Choi, S.J.; Johnson, M.E.; Lehmann, C.U. Data breach remediation efforts and their implications for hospital quality. *Health Serv. Res.* **2019**, *54*, 971–980

23. Neama, G.; Alaskar, R.; Alkandari, M. Privacy, security, risk, and trust concerns in e-commerce. In Proceedings of the 17th International Conference on Distributed Computing and Networking, Singapore, 4–7 January 2016; pp. 1–6

24. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, SwitzerlParlina, A.; Murfi, H.; Ramli, K. Smart city research in Indonesia: A bibliometric analysis. In Proceedings of the 2019 16th International Conference on

Quality in Research (QIR): International Symposium on Electrical and Computer Engineering, Padang, Indonesia, 22–24 July 2019; pp. 1–5.and, 2022

25. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.

26. G. Li, D. Yamaguchi and M. Nagai, “A Grey-Based Decision-making Approach to the Supplier Selection Problem”, Mathematical and Computer Modelling, vo. 46, (2007), pp. 573-781.

27. A. J. Brito, A. T. Almeida and C. M. M. Mota, “A Multicriteria Model for Risk Sorting of Natural Gas Pipelines Based on ELECTRE TRI Integrating Utility Theory”, European Journal of Operational Research, vol. 200, no. 3, (2010), pp. 812-821.

28. M. S. Memon, Y. H. Lee and S. I. Mari, “Group Multi-Criteria Supplier Selection using Combined Grey System Theory and Uncertainty Theory”, Expert Systems with Applications, vol. 42, no. 21, (2015), pp. 7951-7959.

29. V. Baskaran, S. Nachiappan and S. Rahman, “Indian Textile Suppliers’ Sustainability Evaluation using the Grey Approach”, International Journal of Production Economics, vol. 135, no. 2, (2012), pp. 647-658.

30. Jon Glasco Smart Mobility: Challenges and Solutions in Smart Cities, 2019 https://www.beesmart.city/en/solutions/smart-mobility/smart-mobility-challenges-and-solutions-in-smart-cities

31. KyoungJong Park A Risk Management Model for Sustainable Smart City, 2018 International Journal of Advanced Science and Technology

32. R. Souza, M. Goh and F. Meng A Risk Management Framework for Supply Chain Risks, 2007 TLI- Asia Pacific White Papers Series

33. Nam T, Pardo T. Conceptualizing Smart City with dimensions of technology, people, and institutions, 2011 The Proceedings of the 12th Annual International Conference on Digital Government Research

34. Mark Wallin What is smart mobility and why is it important?, 2021 https://www.verizonconnect.com/resources/article/smart-mobility

35. Volodymyr Zavadko Smart Mobility: The Growing Ecosystem of Opportunities, 2022 https://intellias.com/smart-mobility-ecosystem