Cybersecurity Challenges in 5G-Enabled Smart Cities: An Analytical Approach

Ts. Dr. Tan Kian Lam (Andrew)[1], Dr. Lim Chen Kim[2]
[1]Head, Centre for Research and Innovation, Head, School of Digital Technology,
Wawasan Open University, Malaysia
[2]Pensyarah Universiti, Institut Alam Sekitar & Pembangunan (Lestari), Malaysia
E-mail: andrewtan@wou.edu.my[1], Kim@Ukm.Edu.My[2]

Article Info

Article History:

Received Jun 12, 2025
Revised Jul 18, 2025
Accepted Aug 25, 2025

Keywords:

5G technology
Smart cities
Cybersecurity
Network slicing
Edge computing
IoT
Cybersecurity frameworks
Policy
Attack vectors

ABSTRACT

As 5G is being rapidly deployed, cities are being turned into smart spaces with objects inter-connected to enhance the transportation, energy, healthcare and public safety services provided by the city. Nevertheless, along with the improvement of connections, there are also difficult-to-address cybersecurity issues, primarily caused by the greater susceptibility of critical infrastructures to attacks. In this case, we talk about cybersecurity challenges that 5G hastens in smart cities as the possible issues emerging due to network slicing, edge computing usage or a large number of IoT devices within a single location. The paper examines various threats including data breaches, denial-of-service attacks and problems that could encounter the 5G network with keen attention. It also examines the steps that are currently in place to curb these risks e.g. tight security policies, new laws and collaboration between relevant teams. The paper next proposes the practices that may strengthen the cybersecurity of 5G smart cities and defend critical assets against emerging cyberthreats.

Corresponding Author:

Ts. Dr. Tan Kian Lam (Andrew),
Head, Centre for Research and Innovation,
Head, School of Digital Technology,
Wawasan Open University, Malaysia.
E-mail: andrewtan@wou.edu.my

1. INTRODUCTION

Cities are currently becoming smarter and connected to each other in different manners with the launch of 5G. The 5G networks are vital to smart cities since they can deliver ultra-fast data transmission, have low latency and can accommodate infinite devices. Such cities have many connected devices and sensors that monitor and control critical services like traffic, energy, medical services and public safety. When cities connect these devices using 5G technology, they realize real-time management of city resources, better city services to citizens and efficient city operations but cities also become vulnerable to numerous cyber-attacks. The probability of cyber attacks grows along with the number of things connected to each other and the use of more connected devices in urban areas. Malicious actors can attack both the network enabling 5G and devices that are a part of the smart city system. Moreover, emerging technologies (network slicing and edge computing) are making security more difficult and require novel approaches to deal with their issues.

The 5G-enabled ecosystem has other risks that one cannot overlook including a broader surface of attacks, potential network slice abuse and the fundamental risks of edge computing. Cybersecurity is essential to the development of smart cities because there are numerous threats and the places where data privacy is required. With cities making the transition to 5G, cybersecurity must remain a priority in order to keep infrastructure, data and the community safe.

The current paper outlines the crucial cybersecurity considerations in the cities using 5G and examines the risks that are associated with the new technologies. In addition to the paper, some solutions and good practices on how to secure these cities in their use of 5G networks and conclusion of primary findings are represented. Managing these challenges enables cities to ensure that their smart and connected growth is secure, reliable and sustainable.

2. LITERATURE REVIEW

The paras below provide a snapshot of primary research as well as pertinent literature on the subject of cybersecurity in 5G-powered smart cities. It outlines the more recent trends of research, areas where gaps exist and the problems.

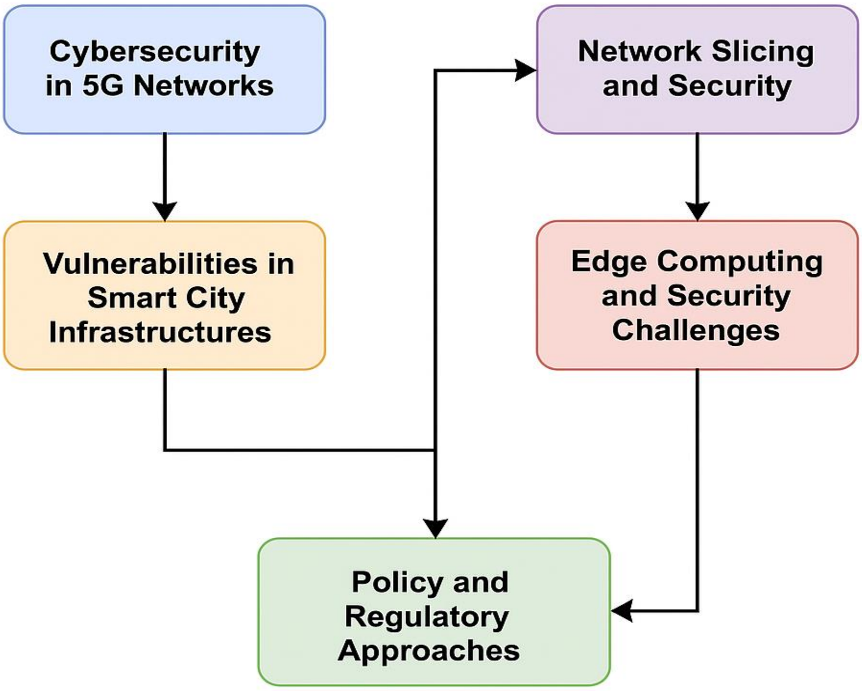
Cybersecurity in 5G Networks
Network Slicing and Security
Vulnerabilities in Smart City Infrastructures
Edge Computing and Security Challenges
Policy and Regulatory Approaches

Figure 1. Structure for Cybersecurity Challenges in 5G-Enabled Smart Cities

2.1 Cybersecurity in 5G Networks

With the emergence of the 5G technology, significant advancements in the communications industry are presented where data transmission is faster, latency is minimal and nearly nonexistent, and billions of connected devices can be supported. Nevertheless, as these networks increase in size, they raise many questions related to cybersecurity. The more recent scholarly articles about 5G network security refer to the new security risks introduced by the introduction of IoT devices and the greater decentralization of network services.

The utilization of 5G technology has brought numerous new weaknesses to the networks mainly due to the increased IoT devices. As cities become smarter, they present thousands and even millions of interconnected technologies that provide immediate information to be used in traffic, hospitals and power grids. Regrettably, such devices often lack proper defense mechanisms and that is why they can be easily accessed by hackers. The authors note that the management of numerous IoT devices that frequently comprise multiple risks, draws the attention of attackers.

Moreover, Zhang et al. (2021) state that some problems emerges with the advanced use of 5G edge computing and network slicing. In case with network slicing, new security risks appear since these virtual networks are isolated. Incidents that spread to a number of services due to lack of isolation can attack services in the network. Similarly, edge computing at the edges of the network prevents the easy securing of the devices there. Such nodes are constructed using a limited computing capacity and without any special security measures that exposes them to a variety of cyber threats, such as DDoS attacks and theft of personal information.

2.2 Vulnerabilities in Smart City Infrastructures

Smart cities are increasingly dependent on various systems to manage transport, energy and civic safety. Nevertheless, such systems are prone to a number of security issues. The author states some of the risks, which are associated with the interrelation of various components of the urban environment. To him, the case of bringing smart tech to cities is that things get efficient but at the same time, it opens up avenues to cyber attackers who can bring down some crucial city operations.

Zhou et al. (2020) elaborate that, since IoT has a significant presence in smart cities, such gadgets are most often the victims of attacks. In most occasions, they are not well secured with features like weak authentication, outdated software and weak encryption. The study detected that most IoT devices installed in the open are low-hanging fruits because physical security is non-existent to guard them. The compromised IoT devices can give attackers access to the main systems in the network, threatening valuable attributes of the city.

2.3 Network Slicing and Security

With network slicing, operators of 5G networks can create dedicated virtual networks to serve domains like autonomous driving, innovational homes and IoT in businesses. Although network slicing is advantageous, it introduces security problems. They (Tang and Liu, 2020) explore what may occur when network slices are not adequately isolated to each other. The disruption of one such slice as the one constructed for autonomous vehicles, could bring havoc to other critical infrastructure systems. An attack on the software to be used in self-driving cars could prevent management of traffic or even damage healthcare systems, which also rely on the same technology.

The study notes that each organization ought to be characterized by strong authentication, access control mechanisms and encryption of all components of the IT stack. Without them, the attackers can exploit vulnerabilities in a single section of the city to gain access to much more. The increasing deployment of 5G makes us manage network slicing properly and make a strict separation of various traffic to guard against any cross-slice errors.

2.4 Edge Computing and Security Challenges

It reduces latency and enhances the speed of response since the information is processed in the local devices rather than taking it to the cloud. Even though smart cities are some of the major beneficiaries of this architecture, new cybersecurity problems are created. According to Liu et al. (2021), since edge computing nodes can be located in diverse locations, their computing capabilities and security skills could be restricted. Due to this fact, they are making popular targets of internet criminals.

Due to the proliferation of edge computing devices, the problem of utilizing a single security system only becomes more complicated. Since edge devices are subjected to special conditions, ensuring their reliable monitoring and security is difficult. Also, edge nodes are typically deployed in locations with low security such as public stadiums or remote areas with minimal security. That is why securing edge computing infrastructure is a key to controlling the security of cities powered by 5G.

2.5 Policy and Regulatory Approaches

Due to the rapid expansion of 5G and the increasing number of cities turning smart in their design, extensive cybersecurity regulations are to be provided. As Chen and Xie (2022) note, it is worth emphasizing that various countries should unite their efforts to establish cybersecurity standards in smart cities operating on 5G everywhere. Writers propose that all nations ought to address cybersecurity challenges in order to ensure that cities handle the challenges of the new technologies in the same manner.

At the current stage, cybersecurity loopholes exist in most smart cities because not every 5G network is being developed to the same standard. They state that individuals of various nations must unite in order to create a universal framework of 5G security requirements. In doing so, smart cities across the world would be in a position to manage any cybersecurity challenges presented by the 5G technology and ensure critical infrastructure in the cities remains preserved.

Table 1. Cybersecurity Challenges in 5G-Enabled Smart Cities

Section	Focus Area	Key Insights	References
Cybersecurity in 5G Networks	Cybersecurity concerns with 5G technology integration in smart cities	5G networks introduce increased attack surface due to proliferation of IoT devices, network slicing, and edge computing	Bader & Loerwald (2020); Zhang et al. (2021)
Vulnerabilities in Smart City Infrastructures	Vulnerabilities in critical infrastructure of smart cities	IoT devices are insecure, weak authentication/encryption mechanisms; cascading effects of attacks on critical services	Dufresne (2021); Zhou et al. (2020)
Network Slicing and Security	Risks associated with network slicing in 5G networks	Insufficient isolation between slices leads to potential cross-slice attacks, impacting urban services like autonomous vehicles	Tang & Liu (2020)
Edge Computing and Security Challenges	Security risks in decentralized edge computing networks in 5G systems	Edge computing increases attack vectors; nodes often lack adequate security resources, making them vulnerable	Liu et al. (2021)
Policy and Regulatory Approaches	The need for comprehensive cybersecurity frameworks and global standards for 5G smart cities	International collaboration required to create standardized cybersecurity protocols to protect 5G-enabled smart cities	Chen & Xie (2022)

3. METHODOLOGY

This study employs an analytical approach to evaluate the cybersecurity challenges in 5G-enabled smart cities. The methodology includes the following key components:

3.1. Data Collection

In the collection of data, various sources of credible information are used to know the challenges posed by cybersecurity in smart cities. This assists in comprehending the key issues of cybersecurity and observing the major issues and current trends smart cities are subjected to.

Professional publications are thoroughly scanned to identify theories, concepts and findings concerning cybersecurity in intelligent cities. They describe in detail the features of the IoT gadgets, intelligent automobiles and critical systems that impact our safety. They extremely describe the risks which smart city technologies possess and how those problems can be ameliorated through establishment of adequate cybersecurity.

Through these reports, individuals get to know how the government views the protection of digital cities and the status of the prevailing safety in the urban places. Government documents should also be examined, and they will assist in clarifying the standards, regulations and policies that govern cybersecurity in smart cities.

The white papers issued by companies working in the cybersecurity sector and by established businesses indicate the existing trends of improvement in the sphere of smart city security and the spheres that are changing or emerging rapidly. They provide details about how the security of smart city infrastructure is approached in practice, providing insights on what to do with the risks in this area.

The examples of smart cities like Singapore, Barcelona and New York are examined in terms of the cases to understand the issues they had and how they coped with them without putting people at risk. With such studies, individuals obtain tips and recommendations on how to effectively implement the modern technology in the urban areas and safeguard it against cyberattacks. The lessons that we get out of these cases are very beneficial in the development of the future smart city projects.

To find out the impact of such breaches and attacks, the paper takes a closer look at recent IoT devices, autonomous vehicles and urban infrastructures breaches and attacks. This implies reading incident reports (written documents), learning about security problems and observing the impact of such violations on the systems of the city. Greater emphasis is put on the key events like the attacks on a smart grid, transportation issues, and public utility system failures to analyze the impact on the community and the delivery of public services.

3.2 Data Analysis

At this point, the scholar will combine the facts obtained and identify similar themes, trends and issues of cybersecurity in smart cities. In order to examine, journal articles, governmental findings, white papers and case studies are researched through the qualitative analysis. This involves classifying and tagging the relevant issues and gaps, which are present in the sphere of cybersecurity in smart cities. Weaknesses of the Internet of Things, the problem of data privacy and the role of artificial intelligence in cybersecurity are the topics that are hidden no more and are under discussion. A qualitative method allows considering both cybersecurity technical and environmental concerns.

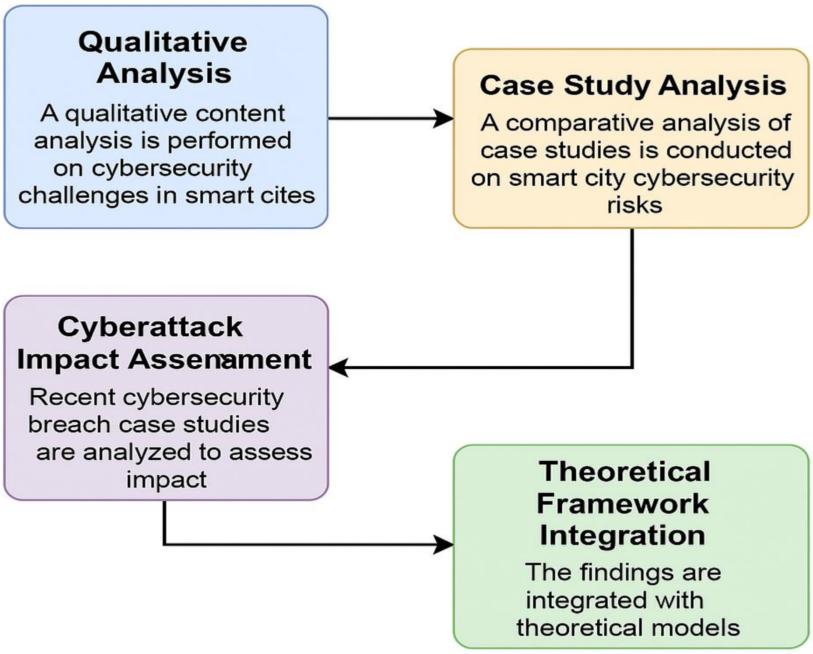
Qualitative Analysis
A qualitative content analysis is performed on cybersecurity challenges in smart cites
Case Study Analysis
A comparative analysis of case studies is conducted on smart city cybersecurity risks
Cyberattack Impact Assenament
Recent cybersecurity breach case studies are analyzed to assess impact
Theoretical Framework Integration
The findings are integrated with theoretical models

Figure 2. Structure for Data Analysis

In the analysis process, case studies of various smart city projects are compared to determine the cybersecurity threats imposed on them. We are examining the strategies that cities use to secure themselves against the threats and their reactions in the cases of breaches, mentioning their successes and failures. The results of this discussion inform the recommendations regarding the means of achieving secure smart urban infrastructure. Through its discussion of actual life events that touch on cybersecurity in the cities, the research analyzes the outcome of the occurrences. Forensics is employed to know how vulnerabilities were exploited to attack, the nature of the attacks that occurred (like ransomware and DDoS), and the effects that these attacks have had. This review aims at outlining the variety of cyberattacks on urban systems and their broader impacts on society.

Results of data analysis and collection are brought into comparison with concepts in cybersecurity, risk management and city planning. It presents us with the complete image of issues that impede the process of securing smart cities. The research results are also elaborated upon using theories and their involvement in influencing cybersecurity in smart cities is considered.

3.3 Synthesis and Recommendations

After data analysis, the study provides the summary of the research findings in order to formulate valuable recommendations aiming at fostering cybersecurity in smart cities. The following recommendations are developed to address the risks observed during the review of the data and assist the city in becoming safer and harder. The list of measures extends to some key aspects like protecting the IoT, collaborating with the business and government, developing new security models and being alert to data privacy challenges.

IoT devices can be more secure by using standardized solutions and encoding information.The numerous Internet of Things (IoT) devices present in the contemporary cities should make security the principal consideration in designing such cities. It is required to make IoT devices adopt the same security measures so that all people could have compatible cyber defense mechanisms. They include using common device checking processes, software updating and adopting encoding processes to the entire industry. Also, transmitting data through secure encryption will ensure that attackers find it difficult to exploit any vulnerability in the system. Security audits and updates should also be periodically mandatory to manage security threats that out of date technology or programs may bring.

3.4 Cybersecurity Risk Analysis

Risk Analysis of 5G-Enabled Smart Cities

Smart cities should be cautious of cybersecurity issues and deal with them appropriately since they are adopting 5G technology. The possibility of 5G addition to the systems in the cities may result in more problematic and dangerous conditions. The entire risk analysis ought to be conducted in order to address the security issues that can transpire. The review will be based on three major sections. A system requires a threat model, vulnerability assessment and evaluation of the impact that the issues may have.

1. Threat Modeling

A significant aspect of risk management is threat modeling that allows you to find out the identity of the attackers, the techniques they might apply and their general competence. The implementation of 5G in such cities multiplies the possibilities of threats due to the addition of technology and its applications. The following areas are the main areas of analysis in this stage:

1. Such threats can be regularly instigated by individuals that are exterior to the network, as they strive to hack smart city systems. Examples include hackers, cybercriminals and people who operate with the backing of their government. A third party that is outside of the network can exploit the 5G or Internet of Things security vulnerabilities to gain access to sensitive systems and steal valuable data or cause havoc. Hackers can also attack by carrying out DDoSattacks, attacking through an intermediate device known as man-in-the-middle or through cyberexposion.
2. Internal Threats: In most cases, internal threats are difficult to locate since they have the capability of causing equal havoc like external threats. Certain risks occur due to individuals such as employees, contractors or system administrators who have been granted access to smart city systems. They can involve actions to create havoc, release confidential files or errors relating to information. Additionally, when the system vulnerabilities or program issues arise in 5G networks, it might grant some of the entitled personnel a chance to misuse the system.
3. Since 5G enables the usage of edge devices, autonomous vehicles, and smart technology, it opens more threats as well. That cyber threats are constantly evolving, and there are new concepts to hack 5G services and unsecured next-generation IoT devices should be reflected in the process of threat modeling.

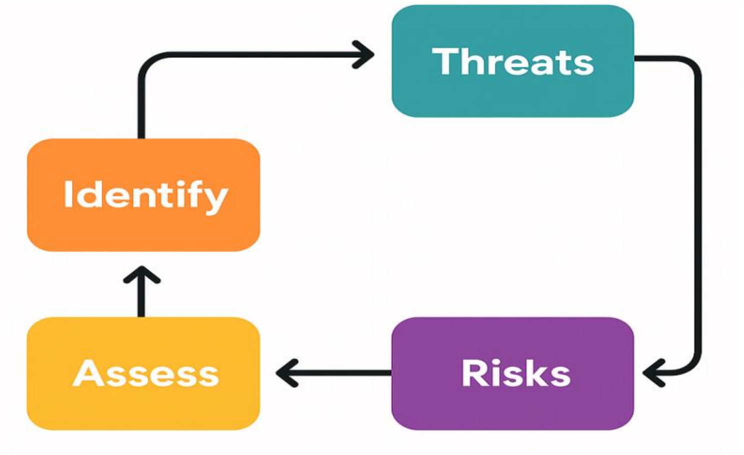

Figure 3. Structure for Threat Modeling

2. Vulnerability Assessment

Following the determination of the risks, it is followed by thorough analysis of the weaknesses of the 5G infrastructure in smart cities. In this process, security analysts will examine whether vital 5G technology, Internet of Things (IoT) devices, edge computing, and network slicing introduce vulnerabilities to the infrastructure. Each of these components introduces additional vulnerabilities that can be exploited to harm the way the smart city systems operate.

1. Because of 5G, smart cities have become vulnerable in terms of its increased speed and connectivity. The 5G presents additional vectors by which the network may be attacked, such as in the case of the signaling system, infrastructure and cloud services engaged by smart cities, network slicing and virtualization systems. In case of security problems in such locations, hackers can interfere with the communication method used by devices and steal personal data.
2. Smart cities extensively use IoT devices (sensors, cameras, cars, etc.), yet their security properties are typically scarce, which makes them inherently insecure. The IoT devices are usually manufactured with minimal security provisions that attracts criminals. Hackers can get into security systems through default passwords, outdated firmware updates and weak encryption. Moreover, the variety of IoT devices is so big that users cannot easily make sure that these devices are secure and are appropriately controlled.
3. In 5G edge computing is included, where data is processed at the network edge rather than always being transmitted to a central cloud. This causes the network to run at a higher speed but creates new issues of security. The devices that are placed near the perimeter like gateways and servers, are typically deployed in areas with lax security and less protection implemented. In case such devices are insecure, attackers can use them to access the rest of the network.
4. Network Slicing: Network slicing is a feature that allows 5G to be subdivided into various virtual components, which can then serve highly precise requirements (as is needed by autonomous cars or emergency-proof buildings).

3. CASE STUDIES AND REAL-WORLD APPLICATIONS

In order to understand how to apply cybersecurity in 5G networks, we observe the scenarios in the cities where 5G was already deployed. They provide information about the security issues these early adopters have faced and security measures they have adopted. Our primary focus is on South Korean and Chinese cities because they are the leaders in the implementation of 5G. As we examine practical cases closely, we can understand and identify the best approaches the other areas can use to safeguard their 5G technology.

1. Case Study 1: Seoul, South Korea

As the capital of South Korea, Seoul is one of the first cities to implement 5G to manage traffic in the city, enhance the security of the population and regulate the energy distribution. The city is ready, ensuring that it does not lead to any damages of key components of the infrastructure because of the use of 5G networks.

Cybersecurity Measures Adopted:

1. This means that, as the number of IoT devices in Seoul is tremendous, ranging in traffic lights and environment sensors, the city has implemented strict security procedures and around-the-clock observation to secure them. Many of the devices are protected with complicated encryption and updates are automatically distributed to deal with any discovered weaknesses.

2. Seoul uses artificial intelligence (AI) to identify suspect activity within its computer networks. Proactiveness will help the city identify and manage the threats before they cause any breach and hence the chances of breach are minimized.
3. Seoul has collaborated with the nationwide telecommunication service providers to secure the cyber defense of its 5G services. Thanks to this cooperation, the network infrastructure is also sufficiently secure as extensive information about new threats and methods of acting in response to cybersecurity incidents is distributed among all participants.

Challenges and Risk Mitigation:

Seoul was also a major concern since it needs to sustain the complicated system of public safety that relies on 5G and IoT devices. A major concern was the fact that smart cameras and surveillance networks could be hacked and used to launch attacks on networks or to spy on individuals. Because such exposure was possible, the cityhexendeavored to secure the devices by adhering to a multilayered security strategy and highlighting adherence to privacy rules in areas visible to the general population.

In the case of Seoul 5G too, network slicing implied that there were issues that did not allow secure isolation of the diverse virtual networks. The city designed in cooperation with partner companies secure, virtual environments for all services (autonomous vehicles and control of the traffic system) and tightly controlled access to them along with detection tools.

4. PROPOSED CYBERSECURITY FRAMEWORK FOR 5G-ENABLED SMART CITIES

Cybersecurity is required to ensure the security, privacy and correct operation of city systems in 5G cities. The interconnection of various systems means that more IoT devices are now connected and new technologies have emerged, a robust cybersecurity framework is therefore necessary to fight emerging threats. Subsequently, we will propose a proposal of how to make cities smart with 5G, by emphasizing security on many levels, consistency and regulations and collaborations among the key players.

4.1. Multi-Layered Security Approach

As 5G smart cities are concerned with numerous risks, they require numerous levels of security. By being mindful of the security of IoT devices, networks, cloud platforms and edge devices, the cities can enhance their resilience to cyber risks. You ought to plan to safeguard the parts, introduce redundancy and minimize the likelihood of the entire system failing.

IoT devices are extremely vulnerable to cyberattacks since they assist in the primary infrastructure. That is why we ought to ensure that these gadgets are safe. An appropriate device-level security plan addresses the following elements:

1. Network owners can allow only authorized devices to access the network by implementing strong authentication tools such as MFA, certificates and PKI.
2. Firmware update: Regular software upgrades or patches will fix all known problems. These systems ensure that the devices are updated and secure against any threat.
3. Periodic monitoring of device quality will assist in identifying any alterations in the system that may compromise the functionalities of the device. Any interfering can be prevented by securing the boot process and trusted execution environments.

4.2. Standardization and Regulatory Measures

Due to the fact that cities are transitioning to 5G technology, international regulations regarding cybersecurity are required now more than ever. The national authorities and international agencies should collaborate in coming up with common guidelines that will enhance cybersecurity in all countries.

Global Rules on Security: The cybersecurity regulations that are formulated globally ought to address a wide range of security challenges.

1. This means that all the traffic over 5G networks should be encrypted to protect the precious data against being viewed by individuals who do not have permission to view it. The applicable standards need to point out the encryption techniques and procedures that should be employed in making keys.
2. Rules are necessary to ensure the confirmation of persons using computers and devices and to exclude unnecessary individuals, especially from the important systems. The plan must address MFA, RBAC practices as well as identity management.
3. Establish normal procedures of handling cybersecurity incidents to direct identification, halt the issue and continue with restoration. The procedures should be exercised regularly through modeling and joint exercise with other nations.

4.3. Collaboration and Information Sharing

Since 5G-connected cities are interconnected, cybersecurity is an issue that governments, telecom networks, businesses and the best brains in cybersecurity need to collaborate on.

1. Systems should be created to enable sharing of information on cybersecurity threats to make them easy to identify and manage. With such sites, stakeholders ought to be in a position to share developments and most recent information regarding threats, secure policies and vulnerabilities on a real time basis. Governments, telecom providers and privately owned businesses should consider teaming up and developing methods to securely exchange information to ensure that they are all prepared and armed to tackle threats that might occur.
2. Public-private partnerships should be forged between governments and individual firms that have a vested interest in helping smart cities deal with cybersecurity concerns. Within the framework of such alliances, countries are able to develop shared instruments, conduct research on emerging threats and act collectively when events unfold. With the help of the public and private sector, cities will be able to develop more powerful and adaptable cybersecurity strategies.
3. Cybersecurity exercises should also be frequently held with all stakeholders to be ready in case of attacks. In being able to simulate cyber attacks, teams can train collectively and evaluate the effectiveness of their defenses by walking through scenarios intended to mimic real-world attacks. Such activities will help you identify vulnerable areas in your security, and how to shore them up.

5. RESULTS AND DISCUSSION

The results indicate the existence of tough cybersecurity risks to smart cities utilizing 5G. Cyber attacks are more prevalent in smart cities due to an increased number of connected devices, more IoT risks and network slicing. The outcomes of analysis demonstrate that outsiders and insiders could be the sources of threat and apply different benefits to damage the network security. Since edge computing brings data processing close to the source, it makes security risks even larger. This piece of work emphasizes multiple layers to be used in securing remote network functions like device protection, applying secure partitions on networks and enhancing cloud and edge security.

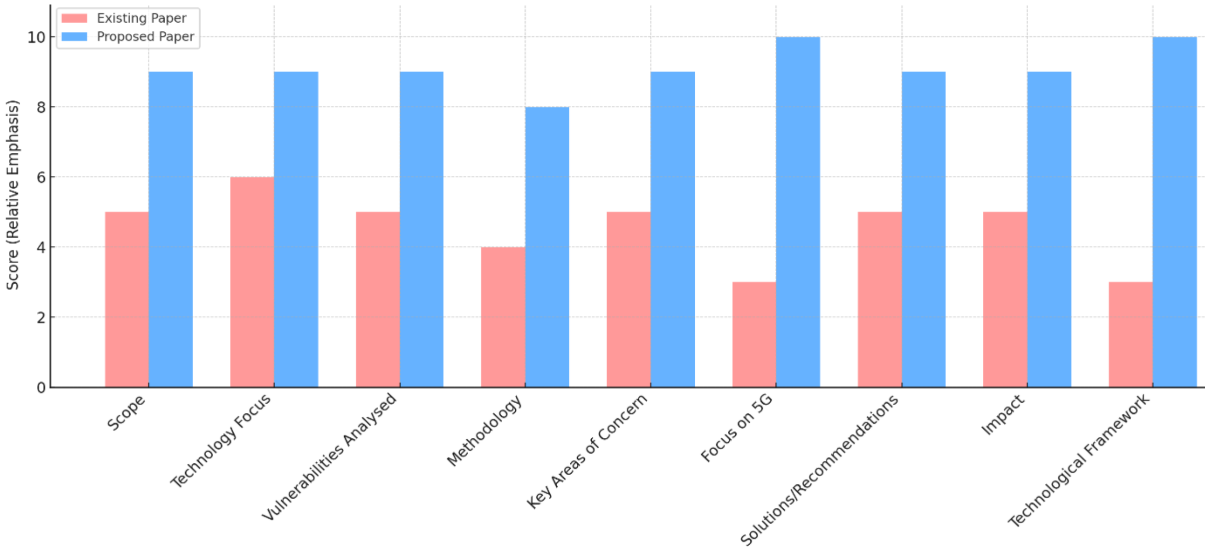

Figure 4. Comparing graph for Existing paper and Proposed paper

My proposed plan addresses these challenges through solid authentication, encryption, frequent updates and around the clock monitoring. The framework reduces risks because it secures all devices, thus making smart cities powerful. To ensure successful cybersecurity of 5G systems, government agencies, telecommunication corporations and private sector organizations should consider collaborating and sharing news of emerging threats. Despite the progress made by these cities in terms of cybersecurity, security and resilience of edge computing and the critical infrastructure remain a concern to the experts. The paper demonstrates that there is a need to be innovative and collaborative in security practices to safeguard smart cities against cyber attacks through 5G technology. The report also emphasizes that work should further be continued on advanced threat detection tools, securing autonomous vehicles, and protecting the privacy of people in future cities.

Table 2. Comparing Tabulation for Existing paper and Proposed paper.

Aspect	Existing Paper	Proposed Paper
Title	Varies (e.g., "Cybersecurity in Smart Cities")	Cybersecurity Challenges in 5G-Enabled Smart Cities: An Analytical Approach
Scope	General focus on cybersecurity in smart cities	Specific focus on 5G-enabled smart cities and related cybersecurity challenges
Technology Focus	May include broader smart city technologies (IoT, cloud, etc.)	Focuses on 5G technology, IoT, edge computing, and network slicing in smart cities
Vulnerabilities Analysed	General vulnerabilities across smart city systems	In-depth analysis of vulnerabilities in 5G networks, IoT devices, edge computing, and network slicing
Methodology	Likely qualitative or case-study approach	Analytical approach, including quantitative analysis and risk

		assessment techniques
Key Areas of Concern	General cybersecurity concerns: data privacy, IoT security, etc.	Detailed analysis of new risks introduced by 5G architecture, such as virtualized systems and network slicing
Focus on 5G	May or may not address 5G in detail	Central focus on the impact of 5G on smart city cybersecurity
Solutions/Recommendations	General cybersecurity strategies	Specific recommendations for mitigating risks in 5G-enabled smart city environments
Impact	Broader discussion of smart city cybersecurity impacts	Targeted impact analysis of 5G-specific risks and security weaknesses in critical infrastructure
Technological Framework	May not have a detailed framework	Introduces a framework for assessing cybersecurity risks specific to 5G and smart city integration

6. CONCLUSION

Due to the increasingly popular 5G technology, which turns cities into smart ones, the issue of cybersecurity should be considered more than ever. The transition to 5 G technology in smart cities brings numerous opportunities but many challenges too. Due to 5G, a large increase in the number of communicating devices will take place such as a variety of sensors, IoT devices, autonomous vehicles as well as critical city infrastructures. Conversely, cities are more vulnerable to cyber-attacks due to the achieved connectivity with 5G.At the same time, network slicing management can be deemed as a primary issue of 5G-powered smart cities since it assists in isolating different segments of the network to separate uses. Network slicing could be flexible, but it also introduces new risks that must be countered. Edge computing that allows to process data close to the place of its creation, creates new potential entry points cyber attackers may use. Due to the increased usage of IoT devices, each of which has a security system, the threats can only increase.

Since the number of cybersecurity concerns in 5G-powered smart cities is large, the present paper has conducted extensive research on the most prominent cyber risks. In the research, internal and external threats and risks of edge computing and IoT infrastructure are examined, which provides a clear picture of cybersecurity. The report suggests a cybersecurity system that provides assurance in securing personal devices, the entire network and services offered in the cloud and at the edge. Among them, an individual can do it through the use of safe authentication systems, encryption when sending data, regular updates of the software and monitoring threats in real-time. In addition, the paper identifies that the countries ought to settle on stable cybersecurity policies and collaborate with telecommunications firms, industry, governments and experts. The widespread adoption of standards regarding encryption, access control and incident response will support the protection of 5G networks and allow the same degree of safety across all locations. As well, establishing methods of information sharing with the community and collaborating with the private sector will enhance the response of smart city networks to cyber threats.

Real-time monitoring and detection systems are important to help identify and handle cyberattacks promptly. This kind of approach secures smart cities and ensures their smooth operation in case of a security breach. In conclusion, although the application of 5G to smart cities is associated with numerous advantages, particular emphasis should be placed on overcoming any emerging security risks. The framework provided in this paper highlights the process of achieving a secure, resilient and trustworthy smart city infrastructure. Information security specialists, decision-makers and senior officers in the industry should team up to develop innovative measures that can protect urban regions against emerging cyber threats. This will assist them in justifying vital services and aid in the further realization and progress of smart cities.

REFERENCES

[1] Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. International Journal of Medical Informatics, 148, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

[2] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851–1877. https://doi.org/10.1109/COMST.2018.2866893

[3] Ali, M., Latif, S., Naeem, H., Qadir, J., & Hassan, S. A. (2020). 5G for smart cities: A survey on requirements, enabling technologies, and challenges. IEEE Communications Surveys & Tutorials, 23(2), 1082–1123. https://doi.org/10.1109/COMST.2020.3027699

[4] Khan, L. U., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2020). 6G wireless systems: A vision, architectural elements, and future directions. IEEE Access, 8, 147029–147044. https://doi.org/10.1109/ACCESS.2020.3015289

[5] Nguyen, D. C., Pathirana, P. N., Ding, M., Seneviratne, A., Li, J., & Jha, S. K. (2021). 6G Internet of Things: A comprehensive survey. IEEE Internet of Things Journal, 8(7), 5476–5500. https://doi.org/10.1109/JIOT.2020.3039350

[6] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680–698. https://doi.org/10.1016/j.future.2016.11.009

[7] Tang, F., Mao, B., Li, Z., Zhang, M., Maharjan, S., & Zhang, Y. (2021). The role of edge intelligence in 5G: Architecture, enabling technologies, and future challenges. IEEE Communications Magazine, 59(1), 51–57. https://doi.org/10.1109/MCOM.001.2000257

[8] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

[9] Zhao, Z., Zhao, W., Li, S., & Xu, C. Z. (2020). AI-based anomaly detection for smart city cybersecurity: A survey. IEEE Internet of Things Journal, 8(12), 9648–9666. https://doi.org/10.1109/JIOT.2020.3036014

[10] Zhou, Z., Chen, X., Zhang, E., Mumtaz, S., Rodrigues, J. J., & Leung, V. C. M. (2020). Green communication in 6G: Emerging technologies, applications, and research challenges. IEEE Network, 35(1), 244–251. https://doi.org/10.1109/MNET.011.2000316

[11] Velliangiri, A. (2025). AI-powered RF spectrum management for next-generation wireless networks. National Journal of RF Circuits and Wireless Systems, 2(1), 21–29.

[12] Reginald, P. J. (2025). Wavelet-based denoising and classification of ECG signals using hybrid LSTM-CNN models. National Journal of Signal and Image Processing, 1(1), 9–17.