Babylonian Journal of Internet of Things
Vol.2025, **pp**. 143–152
DOI: https://doi.org/10.58496/BJIoT/2025/009; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Enhancing Cyber security in Smart Cities: Challenges and Solutions

Wisam K. Jummar [1,*], Osama Khamees Ali [2], Hadeel M. Saleh [1]

[1] *Center for Continuing Education, University of Anbar, Anbar, Iraq.*
[2] *Upper Euphrates Center for Sustainable Development Research, University of Anbar, Anbar, Iraq.*

ARTICLE INFO

Article History

Received 15 Apr 2025
Revised 15 May 2025
Accepted 20 Jun 2025
Published 17 Jul 2025

Keywords

Smart Cities
Cybersecurity
Internet of Things (IoT)
Data Privacy
Blockchain Technologies

ABSTRACT

Leveraging the advanced technologies such as Internet of Things (IoT), Big Data, Artificial Intelligence (AI) and so on, smart cities are a new type of urban model to improve people's quality of life and resource allocation. By all accounts, smart cities — no matter how shiny and hyper connected they may be are on a cyber-odyssey. A lot of threats to data integrity and availability of critical infrastructure are originated from this end like privacy leakage so on. As research objective, this paper mainly intended to investigate the underlying cyber challenges in smart cities comprising vulnerabilities of IoT devices, data privacy issues and no legal codes for governing IT/communications infrastructure. It further suggests generalist solutions, such as the utilization of hybrid security hardware smart secrecy algorithms and machine learning controlled systems for video surveillance/spy camera's or the use of block chain processes used more commonly across all fields. The study provides valuable advice for policy makers, entrepreneurs and practitioners to facilitate the development of smart cities for a safer environment and people as well as plants and animals.

1. INTRODUCTION

Parallel ways of paragraph one: The model of the modern city is they are smart city (the technology and big data on the background) to get cities better quality of life, a more suitable in transportation, energy, health and education. In short, cities apply novel techno-logics (thinking of Internet of Things and the likes) to everything they do day by day - this includes data-driven analysis and decision making. Correct city -An Ideal The ideal of Correct City is designed to solve the urban problem nowadays about a pollution level, over- population and controlling resources relevant to research proved by clear application [1]. The producers try to induce the efficiency of service providers by both public and private nature as well as the reduction in resources use and emissions which are necessary for not destroy environment reducing environment pressure just by producing waste. Healthy life residents Order Under Interdependent services Employment growth In nurturing Digital economy They have got jobs With infrastructure technology high level quality. However, digital applications coverage on following smart systems along with cyber threats is greater than the technology development to guard these kind of platforms for security and safety (Ehteshami et al., 2018; Anthopoulos, 2017), and thus it can be said that cyber security is one fundamental requirement for sustainability in a smart city whose safety could be secured In such a way, security has become one essential point gradually for operations and evolution of smart cities. It requires its difficulties to be reproduced, its non-solutions engaged. Attacking of IoT networks is a big challenge for Smart Cities now; because IOT devices are the inseparable part of smart city based infrastructure they are an open ground for cyber- attacks. "Even if the performances of these works are to take place, they too would be likely to include disruption to public services and bring the city grinding to a halt[2]. in a research report that such attacks could leave cities with cripplingly unusable critical infrastructure. Cloud systems of storage for smart cities security Zugz wang, have made some progress, but store their data on these also has confidentiality and concerns about the real correctness of the integrity. Issues like above are thoroughly addressed in [3], where for example security in cloud systems is analyzed before providing some approaches that might improve resilience and guarantees security. Also, insufficient knowledge of security has caused the threat in terms of users and operators to rise unforeseeable and this was underlined by [4] within his study.Such being needed for an increased awareness especially towards security means against these risks. This implies that there is a clear need to build specific security protocols for the intelligent homes, additionally they identified also in their study of safety risks arising from cloud system data storage and ways to preserve privacy and integrity. Another is "greater awareness and skills training on what safety best practice looks like for smart cities employees and users. Therefore, the underlying message of these studies is straightforward: in line with technological advancements,

*Corresponding author. Email: wisamkhalid6@uoanbar.edu.iq

smart cities need to be established within their digital environment as a black box (i.e., with no need to care about its composition) but also devising all type of strategies for mitigating threats that can disturb it and affect its continuous operation and efficiency".

The aim of this article is to investigate the cyber security-related problems in smart cities and provide a suggestion on how we ought to consider them more secure. Our goal (through exploration): Indent where possible if there are any concerns of there in the 'end citys' If full plans can be provided where everything is on offer that takes into account all inter-linking structure e.g "there are no holes at all over the chain". This study is so important since smart cities are rapidly using more and more advance IT and inter connectivity, thus increasing their chances of being affected by highly disrupting cyber attacks which might even manipulate basic infrastructures like traffic, power or health services. This research is bridging a huge gap of knowledge so we can move that forward to be able to develop the right technology for sustained solutions. This research may be used for governments and policy makers as well, in relation to protecting smart cities over a longer duration. Residents can keep their privacy and data secure, they can protect innumerable residents' own privacy and data. In addition, the displayed function effects are presumably life and economy risk which emerge where production factors are heavily bunched see figure 1

Fig. 1. general smart city

2. LITERATURE REVIEW

2.1. Related Work

The need for smart cities that are resistant, if not impregnable, to cyber-attack is only going to rise with the increase of intelligence in smart technologies. Strong encryption and secure data processing are the key to protecting privacy and security of smart cities (Catton & Ziadali, 2017). They present some solutions for addressing these security loopholes in smart city projects[5]. Similarly, Singhan et al. (2020) introduce a hybrid security architecture to ensure the security of cyber-physical systems and they claimed that their proposed architecture improved data protection and threat detection[6]. As for the fitness of AIbased infrastructure technologies in place for smart cities, a seed is sown in [7] when it comes to machine learning algorithms and anomalies detection systems that can effectively identify and react to emerging threats. Pemasani and Osaka (2021) focus on enhancing cybersecurity on critical infrastructure in smart cities, including transportation, energy and water sectors by considering holistic risk analysis to combat the related threats[8]. Olha et al. (2024)) stress the need of holistic solutions in facing smart cities vulnerabilities initiated by connected devices and call for wider approaches aiding to handle continuously rising threats. [9] Isabieri describes an artificial intelligence-based cyber security Framework block chain-enhanced system for smarter cities with the objective of decreasing the threat levels related to smart city internet of things services (2025)[10]. Finally, Nadella et al. new proposed AI-based generative model architecture for enterprize level data privacy management and found that such multiple techniques finally contributes better in terms of detection of threats, securing the data across the organizations[11]. Together with the

works [14] this highlights a big demand for novel technologies such as AI and hybrid architectures for secure resilient smart city infrastructure.

TABLE I. SUMMARY OF PREVIOUS STUDIES TO ENHANCE CYBER SECURITY IN SMART CITIES

No.	Author	Year	Title	Topic	Methodology	Key Findings	Source
5	Rida Khatoun, Sherali Zeadally	2017	*Cybersecurity and Privacy Solutions in Smart Cities*	Cybersecurity and privacy solutions in smart cities	Review of smart city projects, identification of security gaps	Solutions should include strong encryption and secure data handling	IEEE Communications Magazine
6	Sudhakar Sengan, Subramaniyaswamy V., Sreekumar Krishnan Nair	2020	*Enhancing Cyber-Physical Systems with Hybrid Smart City Cybersecurity Architecture*	Cybersecurity for cyber-physical systems in smart cities	Hybrid cybersecurity architecture to analyze threats and develop secure data environments	Hybrid architecture improves cybersecurity for cyber-physical systems	Future Generation Computer Systems
7	Dinesh Reddy Chirra	2021	*AI-Enabled Cybersecurity Solutions for Protecting Smart Cities Against Emerging Threats*	AI and cybersecurity solutions for smart cities	Use of machine learning algorithms, anomaly detection systems, predictive analytics	AI can identify and mitigate cyber threats effectively	International Journal of Advanced Engineering Technologies and Innovations
8	Praveen Kumar Pemmasani, Motohisa Osaka	2021	*The Future of Smart Cities: Cybersecurity Challenges in Public Infrastructure Management*	Cybersecurity challenges in public infrastructure for smart cities	Cybersecurity risk analysis for urban infrastructure	Increasing cyber threats to transportation , energy, and water systems in smart cities	International Journal of Modern Computing
9	Johnson Sunday Oliha, Preye Winston Biu, Ogagua Chimezie Obi	2024	*Securing the Smart City: A Review of Cybersecurity Challenges and Strategies*	Cybersecurity challenges and mitigation strategies in smart cities	Literature review, analysis of IoT vulnerabilities	Multi-layered solutions are needed to address the growing threats from interconnecte d devices	Open Access Research Journal of Multidisciplinary Studies
10.	Edward Kezron Isabirye	2025	*AI and the Future of Cybersecurity in Smart Cities: A Framework for Secure and Resilient Urban Environments*	AI-driven cybersecurity framework for smart cities	AI and blockchain for enhanced security and data protection	AI and blockchain enhance smart city security by addressing IoT system vulnerabilities	ResearchGate
11	Geeta Sandeep Nadella, Santosh Reddy Addula, Akhila Reddy Yadulla	2025	*Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy Management*	AI-enhanced data privacy management in cybersecurity	Use of generative AI, machine learning, and anomaly detection	Generative AI improves threat detection and data protection in enterprises	Computers

2.2. The relationship between smart cities and cybersecurity

In the main, smart cities rely on digital technology and connected infrastructure to manage their services and improve the efficiency of urban operations. Backed by cybersecurity, therefore, is the continuous operation of these systems-as Adrian Leufu, Executive Director of Embedded Processing Solutions Division at MediaTek, said at an Internet of Things Expo event held in Tokyo in August 2008 the relationship between smart cities and cybersecurity revolves largely around the protection of these networks from cyber threats that may stop services work [12].

The systems used in smart cities, like the Internet of Things (IoT) or big data analytics, need to be protected at highest levels because they have a direct connection to critical infrastructure such as energy, transportation or healthcare on which attacks would disrupt the lives of many people at once [13].
As well, digital expansion in smart cities can make them attractive targets for attackers back - from a desire to steal data and create economic or social damage. In this context, numerous studies stress that there is an urgent need for advanced protection systems to ensure that these systems are not vulnerable to exploitation of flaws .The importance of cyber security in this context involves developing protection systems that can not only resist attacks, but also quickly detect them and respond to them efficiently, as has been confirmed by a number of studies related to cybersecurity within smart cities [14].

2.3. The role of cyber security in a smart city

Cyber security addresses all sorts of practices and technologies to prevent data systems or networks falling victim to attack by viruses and worms, at the same time ensuring that information is confidential secure and available whenever it is needed. It is also known as InfoSec. In the smart city [15] . Cyber how to Cyber The city from attack, it enables the continued operation of its systems and read for this meeting tion that enables it continue serving resident and/or business Prov. Even in the absence of a virus, cyber security needs to be prepared to shield the network from all manner of attacks on applications and systems. In the smart city context, cyber security is involved in shielding the city IT infrastructure to ensure that its online information systems are not compromised by network intruders who may undermine city government. They disturb key facilities, influence the daily life of citizens and they, damage directly the economy if not in an indirect way [16].
Cyber Security Without the security of smart cities targets to those attacking us in many possible forms will be a soft one; (punches and kicks aimed at smart city without a full shield toward back) Blow after blow taking its toll on smart city both business wise, with the way we used to bank once. But for the Internet of Things (IoT) security in such connected ecosystem where a city is not standalone or networked but goes beyond, should be implemented to prevent unauthorized intruders from breaking and manipulating the municipality critical information resources. We also need to think about security when designing a city through technology, not just our good ideas. Time is the only medium by which we can view smart building systems, such as intelligent light and room-control systems that darken rooms not in use or automatically shut off lights if left on out of error, introduce this kind of a minimal hassle scenario. At the same time, smart cities are becoming a trend with regard to their energy saving benefits as increasingly sophisticated building techniques and products have been released to keep history tradition along with eco green. What's more, those sensors and wired and wireless connections establish that cars on city streets can talk to one another: not only pass along positions speed but also the status of a signal light it is as though there were eyes in every part of town all the time keeping track. This kind of on interacting with the system is also forgeable [17].
In contrast, the smart cities process large streams of Big Data from IoT-(Internet of Things) enabled products and services. The latter information is analyzed in order to patterns optimize processes and to base decisions on this knowledge. Even waste management switches which use of resources to consume: Public transport data are for instance used in dependency (e.g., where do users leave the train, whether or not they had a bus change at a transfer station). And also shopping malls gradually tune up there opening hours according to their proximity to neighborhoods, [18].
Artificial Intelligence (AI) is the core technology of smart cities, enabling informed and timely decision-making from data-driven analysis. Artificial intelligence is used in big data analytics on recommending improvements and efficiency, control cyber security by identifying network pattern anomalies and running self-driving cars to improve transport efficiency etc [19].
"Sustainable smart cities" are made possible thanks to new technologies that offer unique opportunities to address urban challenges such as congestion, pollution and natural resource depletion, improving the quality of life in these urban environments.
Cyber threats to the sustainability and security of smart cities are not only serious but also diverse. They include everything from purposeful sabotage of the Internet of Things (IoT) to security breach incidents that try to steal stuff (so far, mostly big data just like before but with a pernicious difference: they are acts not requiring contact by the attacker with its action product all in ways intimately related to absolute operational control! Others still relate to privacy in Cloud Computing and not being able everywhere if not anyone with common sense when security policies must be adhered. In this scenario, the question is to improve cyber security in smart cities and to help them develop a coordinated response against these issues that will lead them towards their stability security[20].

2.4. IoT Networks

In one of such a smart city, equipment with the most commonly used technologies is that related to IoT (Internet of Things) networks, where many connected devices, including sensors like cameras and smart transport systems. But these

nodes are also a major security vulnerability. There are so many devices on there all sorts of things insecure." Most common attacks happening are DoS ones on these networks too, hackers will break into a network with thousands of connected devices and turn them in to a botnet. Then the bombard continuoused as a denial of service attack. In the year 2016 for example, an offence originating from Mirai Botnet was seen which involved the invasion on countless IoT devices and caused a major hindrance in rendering internet services [21].
But that is just one attack vector all of them exploit IoT devices to gain entry, while others are down to malware attacks. The other red flag is those devices using relatively advanced communication protocols, such as MQtt and CoAP, are also suffering from terrible security issues. It is important for IoT devices to be adequately secured using new encryption methods, tough password policies and updated security checks in order for these networks to be defended against [22].

2.5. Data Privacy And Information Security Problems

Smart cities make use of the data which are been provided by devices and digital services to enhance their efficiency and develop new services. But reliance on data also presents a range of privacy and confidentiality challenges. For instance, data are accumulated from the inhabitants but also through smart devices that are attached to the residents without any consent provided by the resident itself and violating its privacy [23].
One problem is inappropriate use of personal data: selling to advertisers or other unreciprocated abuse. "The other half just hate when their conversations are being listened in on and recorded by a company so an ad targeting you to that conversation can be sold because said company should already fucking know how to price that product per canvassing data rather than need for people tell the goddamn piece of companies they're interested in getting the old gutters or the front porch painted, okay? Secure encryption systems, protective regulations of data collection and use as well as clear private terms for privacy protection are the basis for individual data protection [24].

2.6. Vulnerabilities Inside Cloud Systems

Then we enjoys the technique of how to implement different strategies for protecting the security of cloud systems in smart cities with focusing on mainly IOT (Internet of things) devices and other services in view digital information. But those systems often lack the end-to-end encryption protection that would prevent attackers from eavesdropping on data communications. Now, API level there is holes how to get data with no authorization as well. The current identity management and access controls system is also unstable which can lead to security risks. The position taken here is that these concerns may be addressed by existing work in encrypted transmission and storage of data. This will need to be complemented by strong identity management patterns where the identity has to pass through MFA libraries for confirmation and prevent unauthorized access. In addition, cloud service providers should be chosen that comply with international security certification (e.g. ISO 27001) for secure environment [25].
ICS : Iot and SCADA, especially in Smart Cities, as it is a Critical Infrastructure can cause the easiest level of attack. They are what we need to manage our cities and make such complex systems as energy and transportation work, yet they can be hacked. A SCADA system, for example, can cause an entire power grid to come crashing down if successfully targeted by a cyber attack and with devastating economic consequences. It is cyber security subject based on the development of cyber physical systems using information technology for enhancing the efficiency in typical infrastructures e.g., electric power, medical service and transport system which affect to modern society greatly. Depending on obsolete software or lack of security updates to digital systems is similarly hazardous, the author pointed out. The security measures must therefore be kept up to date (keep the roof on), own back-up stop-gaps against cyber-attacks introduced, as well as keep updating training programmers for operation staff in order to maintain surface running and stabile security services already from start Check Point Software Technologies [26].
First of all, Mismatch between demand and Ruler's force for security among Users, Operators is the largest problem facing intelligent city Cyber Security. Some users do not understand how dangerous e-threats (phishing attacks, malware etc.) can be - that is why they are most likely to become potential victims. Operators also have no continuation with training needed to take the right action as the cyber-attack occurs. All users, whether machine or human must be educated over and over again to remind them that cyber espionage is a persistent threat that for the masses; we need to establish a community best practice profile for the prevention of. Mandatory use of MFA for password based access and encouraging users to adopt strong "latest-year" passwords will help secure the systems that attackers exploited holes in [25].

2.8. Guidance for Enhancing Cybersecurity in Smart Cities

Cyber Infrastructure Up gradation One of the crucial requirements for security in smart cities is to upgrade their cyber infrastructure. In the same sense is investing in intrusion detection systems (IDS) and intrusion prevention systems applications (IPS), that monitor activity on network and or system, correlating those activities to signatures so nothing malicious comes into the system. And the initiatives are being built on top of the city's own digital infrastructure to track attacks in real time and deploy to secure if necessary security personnel, should an attack be at hand.

In addition, special cyber-threat monitoring centers are needed that can process data collected from all systems through these methods in a heterogeneous manner in order to monitor the network infrastructure on an ongoing basis. They are also beginning to focus on defending cities from sophisticated cyber-attacks that we generally do not protect our city services for today, e.g., DDoS serving[27].

2.9. Improving responsiveness through past incidents

2.9.1. Design Phase: Build Cyber Security Requirements for Intelligent Systems into Their Design

When it comes to building intelligent systems, concerns about cyber security are so completely integrated into the process from the very beginning that you wouldn't be able to tell just how flat footed intelligent systems would have been in front of the rising wave of cyber-threats right at their early stage development. These can include the identification of necessary security technologies (i.e., encryption, multi-factor authentication or identity management systems). In addition, systems must be continually tested to ascertain their ability to withstand attacks. Comprehensive penetration testing of the systems while not in use at this point must be performed. The aim of such tests is to identify the holes in a company's defences before they become publicized and begin to draw real-world attacks. Types of test would be even emulating an advanced attacks such as DDoS Denial-Of-Service Attack, SQL Injection Scotty-MacKoma and another An American cowboy mission is very effective with these attribute systems can confirm they can take all your New York by air city bear with them city like the City Of The Offenders in Singapore does follow this principle when all smart solutions for the first phase must go on a penetration test hell. They may also allow us the pre-observation of all possible cyber-threats and remove their root cause[28].

2.9.2 Operational phase: Using AI to monitor suspicious activities and applying regular backup methods

And that's where the smart systems come in. Smart cities rely on this artificial intelligence-run surveillance to watch for what might be unusual activity across networks and infrastructure, real-time performance being key. Machine learning learns the abnormal designs. g. the file the upstream-system wants to access is denied/for bidden; one attempts a code page change during load of a write-protected file; not enough free space at destination). "But really one of them all, if not the most important but also what it's worth sharing to others is back up both data and strategies in order to avoid loss or change. If necessary an attack on the system, or its collapse – contingency plans should ensure relatively speedy access to flood relief. City infrastructure service provisioning like the electric services or health-care to a more recent attached connection to the increasing leverage that artificial intelligence is having on Dubai in growing up cities, even if the latter seem with much life as never [29].

2.9.3. Continuous Development Stage: Conduct Security System Performance Assessments periodically and Analyze Past Events

The dynamic evolution phase requires to periodically check the behavior of security systems in order to understand if they continue to perform as required in a dynamic adversarial environment. They have to coincide with the developments of a fringe culture of hackers, if not new worms entirely -- as even out-of-date fables circulated by attackers and background noise on all sides consent. Review of previous incidents has been a key factor in this stage. As such, it seeks to identify potential holes in prior security strategies through an examination of incidences where cyber-attacks already have occurred. Such analytics have been key towards enhancing responses to the next attack in terms of security provision, with leaps forward including increasingly fit-for-purpose security protocols and incorporating new features [14].

Examples: During an evolutionary process, must occasionally assess performance to ensure that security systems continue to perform well in the face of evolving threats. From the fact that it's not just new modified worms, but wholly new postings of modified worms -- much as old myths would bubble up posted by attackers and noise in every direction. Very significant in this step was the analysis of prior events. It can be used to estimate possible limitations of existing security methods by studying examples of cyber-attacks. These analytics have proved to be instrumental in the development of next generation response products for future attack responses, such as enhancements to: security scalability (better use of protocol techniques), and addition of new modes [14].

In Estonia this analysis of incident is made to test functioning of security systems and technology on the raw level of city space, can work the future for smart city in future [2]. Smart City of three stages (design, application and continuous improvement) can assist in creating a secure surrounding for business world. These stages guarantee that smart systems will never be defenseless from the beginning to the end throughout proactive characterization to resist new threats. [30].

2.10. A Smart Dubai City

In Dubai, the most remarkable and modern example in Middle East region to increase protections on digital security -in particular the IoT devices- is a cyber security of things digital technology center. The center's primary task is to monitor threats to smart grids, which include sewage pumping stations in this city's electricity and when they do happen, help people respond as rapidly as possible once an attack has taken place. Simultaneously it gathers and analyzes data on these threats in real-time using an AI based graphical analytics tool it developed at Columbia University to monitor different layers of networks for abnormal behavior. It use of smart monitoring tools installed across a city all hours when a city is attacked, and when the data from systems service various companies aggregates to monitor for suspicious activity in this condition that indicates someone is about to try and operate. It would base to a large extent (early warning and real-time analysis of cyber-attacks based on technology even as AI for the general aspect but with also cause response aspects concerning distributed denial-of-service (DDoS) attacks and the functionality of DDoS type attack which can be utilized by state institutions themselves for example in transport networks or power grids. It also has rapid reaction systems which it says are designed to "neutralize" any attack in cyberspace before it happens by using immediate, retaliatory measures on the ground. Through this center, the emirate will secure its digital infrastructure and confront cyber threats of today. It will emerge as an example safe smart city for the world[30].

Fig. 2. Dubai smart city

A security scheme around this template has since been playing out in Singapore too – one that has passed all litmus tests and every inch of qualification pressure Buddhists to have affixed theirs for "quality assurance". This way all phases can be seen as an element in a system of quality so that it complies with international standards and even to make the experience enjoyable for those organizations which are passionate about ISO 27001. Except the identical fence provisions above, all of the requirements for the security of electronic information and computer equipment shall apply to whole PNG in Shenyang City. And this has only deepened the dependence of God's own Kingdom on interference-free China for every stage of customer. It also helped consolidate Chinas credibility of non-interfering on delivery services to customer at all levels by digital means. Such protection would cover data as well as systems and span the entire city — encouraging better cyber security and availability in digital services provided. Singapore's Smart City. Integration of cyber security in energy infrastructures, smart lightning network and Internet of Things [31].

Fig. 3. Singapore city

Tallinn in Estonia is one of the most important smart cities that features cyber within its technology landscape. Estonia has a very good defences and not going to let it electronic systems; systems go down just like that. Estonia is also one of the best examples in e-government and using technology for the efficiency of its state services, such as provides education or health care and e-government application. Such things should be done:
Estonia leverages modern mechanisms, including block chains to secure integrity of data. Also, all informant ion exchanged on government networks are encrypted with strong encryption algorithms to maintain security. And there were also broadened policies that were put in place, for citizens to increase the level of security in helping them training programmers on phishing like attacks with advice against them and how to protect their personal information as we live more silent generation. The international partnership between Estonia and the EUs, as well with others in cyber security system and sharing of information or data on the threatened infected systems to give a common response to these threats makes us increase our favor among intelligent people. These combined measures have made Estonia one of the safest places in the world to use such electronic services from government, which are also an optional feature for individuals (some even available for children) some offers like social security payments or buying transport tickets. It protects all data entered into such systems from being singled out and attacked. [32] As can be observed in this photo, by consolidating disparate digital data sources such as those from IoT sensors, urban lighting systems, or commuting and social and public services into an interconnected system of systems individual pieces rather than looking at the entire picture), Tallinn Estonia has emerged as a illuminated city where not an ounce of energy is wasted figure 4.

Fig. 4. Estonia city

2.11. Road Map for Strengthening Cybersecurity in Taiwanese Smart Cities

Tallinn in Estonia is one of the most important smart cities that features cyber within its technology landscape. Estonia has a very good defences and not going to let it electronic systems; systems go down just like that. Estonia is also one of the best examples in e-government and using technology for the efficiency of its state services, such as provides education or health care and e-government application. Such things should be done:
Estonia leverages modern mechanisms, including block chains to secure integrity of data. Also, all information exchanged on government networks are encrypted with strong encryption algorithms to maintain security. And there were also broadened policies that were put in place, for citizens to increase the level of security in helping them training programmers on phishing like attacks with advice against them and how to protect their personal information as we live more silent generation. The international partnership between Estonia and the EUs, as well with others in cyber security system and sharing of information or data on the threatened infected systems to give a common response to these threats makes us increase our favor among intelligent people. These combined measures have made Estonia one of the safest places in the world to use such electronic services from government, which are also an optional feature for individuals (some even available for children) some offers like social security payments or buying transport tickets. It protects all data entered into such systems from being singled out and attacked. [32-33] As can be observed in this photo, by consolidating disparate digital data sources such as those from IoT sensors, urban lighting systems, or commuting and social and public services into an interconnected system of systems (a individual pieces rather than looking at the entire picture), Tallinn Estonia has emerged as an illuminated city where not an ounce of energy is wasted figure 4.

3. CONCLUSION

Cybersecurity is a key pillar for the success and sustainability of smart cities. Incorporating technologies such as the Internet of Things and artificial intelligence into city management creates significant opportunities, but opens the door to

security challenges that threaten critical infrastructure and essential services. Key challenges include poor security of IoT devices, data privacy issues, and lack of appropriate legislation.

To address these challenges, it requires the adoption of multidimensional solutions that include the application of strong encryption standards, the use of AI-powered surveillance systems, the strengthening of legislative frameworks, and the exploitation of blockchain technologies to ensure data security. Through these efforts, governments and stakeholders can protect smart cities from cyber threats, ensuring the continuity of vital services and enhancing public confidence in these future cities. Success in smart cities is not only linked to technological progress, it depends on striking a balance between innovation and safety.

Conflicts Of Interest

The paper states that there are no personal, financial, or professional conflicts of interest.

Funding

The absence of any funding statements or disclosures in the paper suggests that the author had no institutional or sponsor backing.

Acknowledgment

The author acknowledges the support and resources provided by the institution in facilitating the execution of this study.

References

[1] D. Chen, Z. Wawrzynski, and P. Lv, “Cyber security in smart cities: A review of deep learning-based applications and case studies,” Sustain. Cities Soc., vol. 66, p. 102655, 2021.
[2] D. B. Rawat and K. Z. Ghafoor, Smart Cities Cybersecurity and Privacy. Elsevier, 2018.
[3] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, “A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities,” Sustain. Cities Soc., vol. 50, p. 101660, 2019.
[4] D. B. Rawat, R. Doku, and M. Garuba, “Cybersecurity in big data era: From securing big data to data-driven security,” IEEE Trans. Serv. Comput., vol. 14, no. 6, pp. 2055–2072, 2019.
[5] Z. Lv, D. Chen, R. Lou, and A. Alazab, “Artificial intelligence for securing industrial-based cyber–physical systems,” Futur. Gener. Comput. Syst., vol. 117, pp. 291–298, 2021.
[6] J. Laufs, H. Borrion, and B. Bradford, “Security and the smart city: A systematic review,” Sustain. Cities Soc., vol. 55, p. 102023, 2020.
[7] H. H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, Cyber-Physical Systems: Foundations, Principles and Applications. Morgan Kaufmann, 2016.
[8] M. Batty et al., “Smart cities of the future,” Eur. Phys. J. Spec. Top., vol. 214, no. 1, pp. 481–518, 2012.
[9] M. Antonakakis et al., “Understanding the mirai botnet,” in Proc. 26th USENIX Security Symp. (USENIX Security 17), 2017, pp. 1093–1110.
[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Comput. Netw., vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.
[11] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the Internet of Things: Threats and challenges,” Secur. Commun. Netw., vol. 7, no. 12, pp. 2728–2742, 2014, doi: 10.1002/sec.795.
[12] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013.
[13] P. K. Pemmasani and M. Osaka, “The future of smart cities: Cybersecurity challenges in public infrastructure management,” Int. J. Modern Comput., vol. 4, no. 1, pp. 72–85, 2021.
[14] J. S. Oliha, P. W. Biu, and O. C. Obi, “Securing the smart city: A review of cybersecurity challenges and strategies,” Eng. Sci. Technol. J., vol. 5, no. 2, pp. 496–506, 2024.
[15] B. Hamid, N. Z. Jhanjhi, M. Humayun, A. Khan, and A. Alsayat, “Cyber security issues and challenges for smart cities: A survey,” in Proc. 13th Int. Conf. Math., Actuarial Sci., Comput. Sci. Stat. (MACS), 2019, pp. 1–7.
[16] A. Khan, N. Z. Jhanjhi, and M. Humayun, “The role of cybersecurity in smart cities,” in Cyber Security Applications for Industry 4.0, Chapman and Hall/CRC, 2022, pp. 195–208.
[17] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, and J. Al-Jaroodi, “Applications of big data to smart cities,” J. Internet Serv. Appl., vol. 6, no. 1, pp. 1–15, 2015.
[18] I. A. T. Hashem et al., “The role of big data in smart city,” Int. J. Inf. Manage., vol. 36, no. 5, pp. 748–758, 2016.
[19] M. J. Reis, “AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities,” Electronics, vol. 14, no. 12, p. 2492, 2025.

[20] D. R. Chirra, "AI-enabled cybersecurity solutions for protecting smart cities against emerging threats," 2024.
[21] D. Kim, S. Jeon, J. Shin, and J. T. Seo, "Design the IoT botnet defense process for cybersecurity in smart city," Intell. Autom. Soft Comput., vol. 37, no. 3, 2023.
[22] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, and S. Karuppayah, "MQTT vulnerabilities, attack vectors and solutions in the Internet of Things (IoT)," IETE J. Res., vol. 69, no. 6, pp. 3368–3397, 2023.
[23] S. Mirishli, "Ethical implications of AI in data collection: Balancing innovation with privacy," arXiv preprint arXiv:2503.14539, 2025.
[24] D. Helbing et al., "Ethics of smart cities: Towards value-sensitive design and co-evolving city life," Sustainability, vol. 13, no. 20, p. 11162, 2021.
[25] F. J. G. Arellano et al., "Examining cybersecurity culture in Leon city organizations: Insights from 2022," Ingeniare: Rev. Chil. Ing., vol. 32, pp. 1–16, 2024.
[26] N. Tatipatri and S. L. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security," IEEE Access, vol. 12, pp. 18147–18167, 2024.
[27] N. Alsabilah, "Adaptive cyber security for smart home systems," Ph.D. dissertation, Howard Univ., 2024.
[28] M. El Khatib, M. Alhammadi, and A. Almulla, "Attributes of smart education in smart cities," Int. J. Bus. Anal. Secur. (IJBAS), vol. 4, no. 2, pp. 157–178, 2024.
[29] S. Ahmed, M. F. Hossain, M. S. Kaiser, M. B. T. Noor, M. Mahmud, and C. Chakraborty, "Artificial intelligence and machine learning for ensuring security in smart cities," in Data-driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances. Cham: Springer Int. Publishing, 2021, pp. 23–47.
[30] M. A. I. Mallick and R. Nath, "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments," World Sci. News, vol. 190, no. 1, pp. 1–69, 2024.
[31] H. Singh, "Cybersecurity for smart cities protecting infrastructure in the era of digitalization," SSRN, p. 5267856, 2025.
[32] C. Anschütz, "Towards long-term use of information systems: Investigations into the design of smart mobility systems to improve smart cities," Ph.D. dissertation, FernUniversität in Hagen, 2024.
[33] N. Jeffrey, Q. Tan, and J. R. Villar, "A review of anomaly detection strategies to detect threats to cyber-physical systems," Electronics, vol. 12, no. 15, p. 3283, 2023.