Contents lists available at ScienceDirect

Journal of Innovation & Knowledge

journal homepage: www.elsevier.com/locate/jik

Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity

Heng Zeng [a,b,*], Manal Yunis [c], Ayman Khalil [c], Nawazish Mirza [d]

[a] *Business School, Hubei University, Wuhan 430062, China*
[b] *Open Economy Research Center, Wuhan 430062, China*
[c] *Department of Information Technology and Operations Management, Adnan Kassar School of Business, Lebanese American University, Beirut, Lebanon*
[d] *Excelia Business School, CERIIM, France*

ARTICLE INFO

JEL Codes:
O31
Q55
R11

Keywords:
Cybersecurity
Smart cities
IoT
AI-driven anomaly detection
Human factors
Technological readiness

ABSTRACT

As smart cities advance, Internet of Things (IoT) devices present cybersecurity challenges that call for innovative solutions. This paper presents a conceptual model for using AI-enabled anomaly detection systems to identify anomalies and security threats in smart city IoT networks. The foundation is supported by the Complex Adaptive Systems (CAS) theory, Technology Acceptance Model (TAM), and Theory of Planned Behavior (TPB). In this framework, the importance of user engagement in ensuring effective AI-driven cybersecurity solutions is underlined with an emphasis on technological readiness and human interaction with AI. By fostering a security-conscious culture through continuous education and skills development, this research provides actionable insights for enhancing the resilience of smart cities against evolving cyber threats. The proposed framework lays the groundwork for future empirical studies and offers practical guidance for policymakers and urban planners dedicated to safeguarding the digital infrastructures of potentially tomorrow's cities – the smart cities.

Introduction

Urbanization and modern technological advancement are the hallmarks of this era, with the term "smart cities" symbolizing contemporary life. The concept was born out of a unique integration of digital technologies into urban infrastructures at the beginning of the 21st century. The utilization of cutting-edge technology in smart cities targets multiple main objectives, like economic development, efficient public services, sustainable urban planning, and citizen engagement (Sharma, Haque & Blaabjerg, 2021). This has been achieved by utilizing diverse technologies across sectors such as energy management (Shu, Wang, Umar & Zhong, 2023), transportation infrastructure (Umair, Cheema, Cheema, Li & Lu, 2021), financial technology (Liu, Su, Tao, Qin & Umar, 2024) and governance (Makpotche, Bouslah & M'Zali, 2024)). An illustration of smart cities is depicted in Fig. 1 (Ma, 2021).

The Internet of Things, a network of interconnected devices and sensors, is central to this transformation as it promises to change how people live in cities (Shehadeh, Hussainey, Alhadab, & Kilani, 2024; Hashem et al., 2016). Nonetheless, as IoT technology proliferates, it brings numerous cyber security challenges that require robust, innovative solutions. The widespread presence of diverse IoT devices in urban settings significantly improves city management and citizens' experiences, thus contributing to increased energy efficiency, better traffic management, public safety and overall quality of life (Rehan, 2023). This integration has also led to the growing complexity of urban networks, making them more vulnerable to cybersecurity risks (Hoppe, Gatzert & Gruner, 2021; Rangu et al., 2024).

According to Konstantopoulou, Sklavos and Ognjanovic (2023) and Wu, Han, Wang and Sun (2020), the IoT networks necessary for smart city infrastructures have various devices, each with different protocols and security levels. This diversity increases its usefulness but also exposes it to security risks because some devices do not have proper security mechanisms or manage sensitive data. This configuration makes it attractive to hackers since an attack on one device would result in other network components being affected too (Rehan, 2023; Demertzi, Demertzis & Demertzis, 2023). For example, one can see from Fig. 2 how any compromise on a smart city component could negatively impact others.

Given the scale and diversity of IoT deployments, traditional cybersecurity techniques, typically designed for smaller and more homogeneous networks, are insufficient (Huber, Kandah & Skjellum, 2023). The sensitivity of the data handled by IoT networks further

[*] Corresponding author.
E-mail addresses: myth3085@sina.com (H. Zeng), myunis@lau.edu.lb (M. Yunis), ayman.khalil02@lau.edu.lb (A. Khalil), elahimn@excelia-group.com (N. Mirza).

https://doi.org/10.1016/j.jik.2024.100601
Received 15 July 2024; Accepted 15 October 2024
Available online 5 November 2024

exacerbates these vulnerabilities, with potential consequences ranging from privacy invasions to disruptions of critical services (Roman, Zhou & Lopez, 2013; Sicari, Rizzardi, Grieco & Coen-Porisini, 2015). The rapid expansion of IoT networks, with over 25 billion active devices as of 2020 and projections exceeding 75 billion by 2025 (Vailshery, 2023), underscores the urgency of addressing these security challenges. Indeed, IoT cyberattacks more than doubled in a single year, rising from approximately 639 million in 2019 to over 1.5 billion in 2020 (Cyrus, 2021), and the number of IoT devices, such as smart home devices and routers, is projected to exceed 29 billion by 2030 (Kaspersky, 2023).

In light of these growing threats, Artificial Intelligence (AI) can potentially contribute to addressing this issue through anomaly detection, which is vital for identifying and mitigating cyber security threats (de Azambuja et al., 2023; Ahmed, Mahmood & Hu, 2016). IoT network cybersecurity can be highly improved by AI-based techniques that identify complicated patterns and analyze large volumes of data (Liu, Zhang & Zhou, 2018). For example, machine learning models might be able to recognize unusual patterns or behaviors in network traffic that may signify a cyberattack (Xu, He & Li, 2014). Table 1 lays out how AI stands superior to traditional cybersecurity methods.

AI capabilities are particularly valuable in smart city contexts because they can prevent major disruptions by rapidly detecting and responding to security concerns (Mehta, Pandit & Modi, 2020). Nevertheless, despite the promise of AI, there is a big void in the literature regarding comprehensive frameworks systematically outlining how AI could be used in anomaly detection for IoT networks in smart cities. The gap poses a crucial hurdle for cities wanting to harness AI for better cyber-security, as there is limited guidance on implementing and optimizing these technologies within intricate urban environments (Ferrag et al., 2018; Zhang, Deng, Liu, Zheng & Mahmood, 2019).

To address this gap, the study presents a conceptual model that elucidates how artificial intelligence (AI) might bolster the cybersecurity of Internet of Things (IoT) networks in smart cities. This model is grounded in various fundamental theoretical viewpoints, notably Complex Adaptive Systems (CAS) theory (Holland, 1995). CAS theory conceptualizes smart cities as dynamic systems comprising interconnected and interdependent components that autonomously adjust in response to environmental changes. Moreover, the Technology Acceptance Model (TAM) (Davis, 1989) and Theory of Planned Behavior (TPB) (Ajzen, 1991) are employed to investigate how stakeholders' perceptions and intentions affect the adoption of AI-driven solutions. Furthermore, Socio-Technical Systems (STS) theory (Trist, 1981) is applied to understand how technology interacts with social factors in deploying AI in smart city security. Based on the above, this study seeks to answer the following research questions:

1. **RQ1:** How do AI-driven anomaly detection techniques (independent variable) impact cybersecurity (dependent variable) in smart city IoT networks?
2. **RQ2:** What role does technological readiness (moderating variable) play in the relationship between AI-driven anomaly detection and cybersecurity in smart city IoT networks?
3. **RQ3:** In what way do human factors (mediating variable) influence the effectiveness of AI-driven anomaly detection in enhancing cybersecurity in smart city IoT networks?

Based upon these research questions, the motivation behind this study stems from the urgency to enhance cybersecurity in smart cities through the efficient employment of AI-driven anomaly detection systems. As highlighted earlier, the identified gap in the extant body of literature underscores the need for a holistic framework that addresses the unique challenges of IoT networks in urban environments. Hence, the objective of this study is to fill this gap by proposing a conceptual model on how AI-driven anomaly detection systems can improve IoT network security in smart cities.

Moreover, the main significance of this study lies in its twofold emphasis on theoretical analysis and practical application. First, it delves into AI-driven cyber security challenges and opportunities in smart cities, giving insights into how these technologies can be optimized based on urban settings. Second, the research offers an operational roadmap for practitioners, defining the stages and best practices which could be adhered to when implementing artificial intelligence models to real life smart city scenarios. This roadmap is designed to be actionable, providing cities with the tools they need to enhance their cybersecurity posture in the face of evolving threats. This is anticipated to provide useful insights to practitioners responsible for securing smart cities.

The remainder of this paper is organized as follows: the following section provides a thorough analysis of the current body of literature, specifically focusing on the current state of artificial intelligence in the topic of cybersecurity with an emphasis on anomaly detection in IoT networks within smart cities. Next, the relevant theoretical frameworks are introduced. The paper then presents the proposed conceptual model, examining the relationships and potential impacts of the highlighted elements in the context of smart cities. The discussion then shifts to the implications of the framework, considering its theoretical and practical implications for stakeholders engaged in technology and urban development. Finally, the study's contributions to advancing AI-driven cybersecurity strategies in smart cities are summarized, along with a discussion of limitations and suggestions for future research.

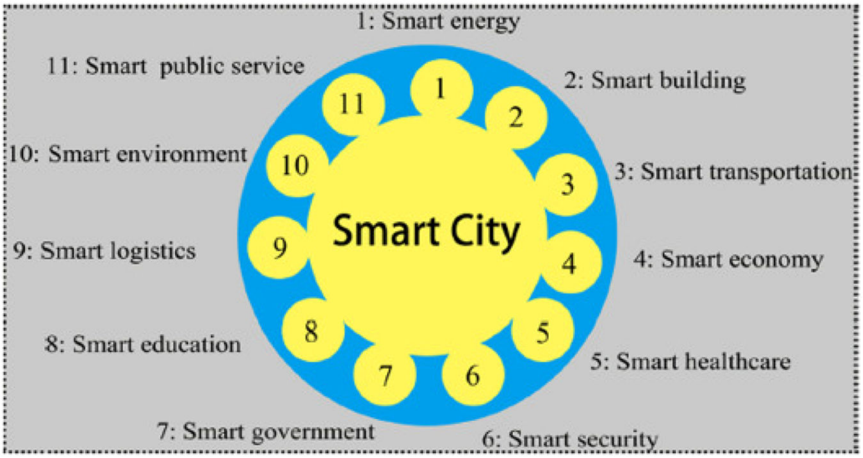

Fig. 1. Smart city components illustration.
Source: Ma (2021).

Literature review

This research looks into the changing field of AI-driven anomaly detection, an area that plays a crucial role in addressing cybersecurity concerns in IoT networks within smart cities. It begins by looking at how important IoT is in urban areas and provides insight into the complexities it poses. The focus then moves to cyber security in smart cities which has become increasingly relevant because of the rise of cyber threats. Artificial intelligence is thus addressed next with anomaly detection techniques designed to enhance cybersecurity. Finally, this literature review paves the way for the subsequent development of a conceptual model that seeks to combine all these strands into a coherent understanding of AI-driven anomaly detection in IoT networks within Smart Cities.

Smart cities and the role of IoT

With the integration of digital technology into the urban fabric, the notion of "smart cities" has emerged as a critical response to the challenges posed by urbanization (Ejaz & Anpalagan, 2019). These cities aim to improve sustainability, operational efficiency, and quality of life by combining technology, infrastructure, and urban planning (Shahidehpour, Li & Ganji, 2018).

As smart cities have evolved, they have become dynamic ecosystems characterized by increasing complexity and capacity (Linde, Sjödin, Parida & Wincent, 2021). Initially focused on specific technological implementations, smart cities now encompass a wide range of applications and services driven by the goals of sustainability, citizen welfare, and economic development (Neirotti, De Marco, Cagliano, Mangano & Scorrano, 2014). Central to this technological revolution is the Internet of Things (IoT), which plays a crucial role in the development of smart cities. IoT integrates sensors and connectivity into physical objects and infrastructure to collect and exchange data, serving as the engine for intelligent city services and operations (Hashem et al., 2016). The applications of IoT in smart cities are diverse, ranging from energy management smart grids to traffic and transportation systems that optimize flow (Alaba, Othman, Hashem & Alotaibi, 2017). This variety demonstrates how adaptable and far-reaching IoT technology is in urban settings (Sharma & Jain, 2023).

However, the integration of IoT technologies presents significant challenges, particularly in terms of privacy, security, and data management (Elmaghraby & Losavio, 2014; Al-Turjman, Zahmatkesh & Shahroze, 2022). To safeguard this complex network of devices and data from cybersecurity threats, strong and sophisticated security solutions are required (Lu, Xu & Xu, 2018).

Table 1
AI advantages over traditional cybersecurity methods.

Proactive Detection	Unlike conventional rule-based systems, AI uses machine learning to identify unexpected dangers.
Adaptive Learning	AI upgrades its knowledge of assault patterns on a regular basis.
Analysis of Behavior	AI recognizes anomalies in behavior and distinguishes departures from the norm.
Identification of Patterns	Even under disguise, AI is able to identify intricate assault patterns.
Reduced False Positives	Decreased False Positives: AI improves threat identification, reducing the number of false alarms.
Dynamic Response	AI makes quick decisions in response to threats.
Threat Hunting	AI actively looks for undiscovered dangers.
Forecasting and Avoidance	AI anticipates dangers so that preventative measures can be taken.
Scalability	AI analyzes massive amounts of data effectively.
Acquiring Knowledge from Experience	AI gets better with time as a result of previous events.
Handling Complexity	AI handles complexity by coordinating several attack tactics.
Reduced Human Biasedness	Reduced Human Bias: AI offers unbiased danger evaluations.

Source: Adapted from Singh (2023).

Cybersecurity challenges in smart city IoT networks

IoT networks, essential to the infrastructure of smart cities, present significant risks due to their scale and diversity. These networks comprise a wide range of devices with different security protocols and varying degrees of vulnerability (Sharma & Jain, 2023; Lu et al., 2018). Consequently, the diversity in these devices adds to the richness of functionality in smart cities but also introduces numerous potential security vulnerabilities.

The widespread connectivity of IoT networks, while facilitating data flow and integration crucial for smart city operations, also opens up numerous cyberattack opportunities. These vulnerabilities are exacerbated by the disparate security protocols across devices, where less secure devices may act as gateways to compromise the entire network (Alaba et al., 2017; Roman et al., 2013).

Moreover, the integration of digital networks with physical infrastructure in smart cities introduces dual risks. Cyberattacks can impact vital city services, leading to immediate physical consequences (Demertzi et al., 2023). For instance, an attack on traffic management systems could cause widespread disruptions, delay emergency

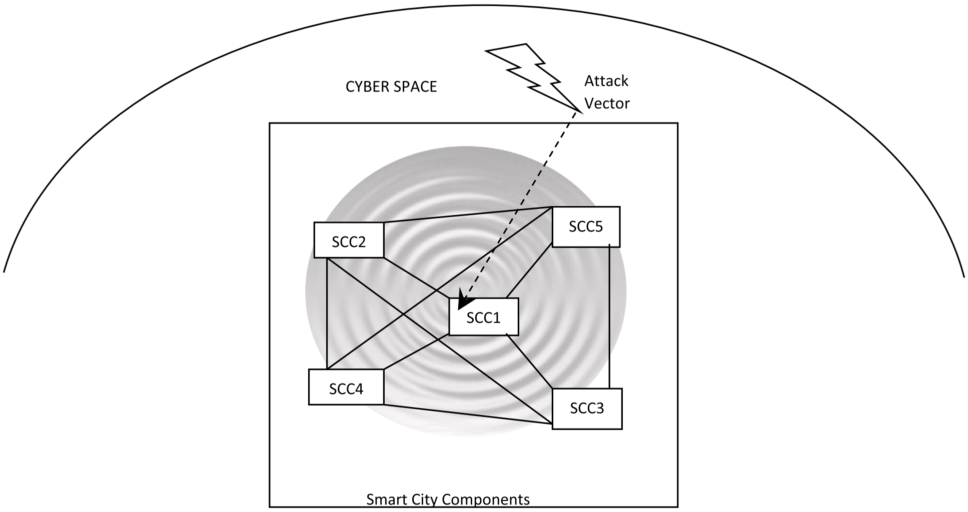

Fig. 2. Cyberattack impact on smart city components (SCC).

responses, and even result in accidents. Similarly, attacks on utility networks could lead to service interruptions and safety hazards, significantly affecting daily life for city residents (Sicari et al., 2015). Standard cybersecurity solutions may not be adequately prepared to handle the physical effects of digital breaches, which poses a significant challenge (Granjal, Monteiro & Sa Silva, 2015).

A 2019 article by Deloitte highlighted three key factors influencing cyber risk in smart city ecosystems (Pandey, Golden, Peasley & Kelkar, 2019):

1. The merging of the virtual and physical worlds due to the convergence of information technology and operational technology, blurring the divide between physical and cyber domains;
2. Compatibility issues between new and legacy systems, given the coexistence of old and new technologies in smart cities; and
3. The integration of various city services and supporting infrastructure, facilitated by IoT and diverse digital systems and technologies. This last factor is depicted in Fig. 3.

Prominent cyberattacks, such as the Mirai botnet, have demonstrated the potential for IoT-targeted attacks to cause extensive disruption. The attackers launched massive distributed denial-of-service (DDoS) attacks by controlling thousands of IoT devices (Ashraf, Tahir, Habaebi, & Isoaho, 2023). Such incidents highlight the extensive damage IoT vulnerabilities can cause, including the disruption of internet services, and emphasize the critical need for strong cybersecurity measures in smart city infrastructures (Antonakakis et al., 2017). Another example is the Emotet virus, which infiltrated the city administration of Allentown in 2018. Emotet, originally a banking trojan, evolved to steal network passwords, financial information, address books, and perform DDoS attacks. It propagated through malicious scripts attached to emails, severely disrupting government activities in Allentown by infecting nearly every system and causing major disruptions to traffic and tax collection systems, among other areas (Blake, 2018).

AI-Driven anomaly detection in cybersecurity

Artificial Intelligence (AI) significantly enhances efficiency and decision-making across various sectors. However, AI adoption also introduces new risks and challenges. For example, a recent article investigated how AI can be incorporated into renewable energy systems and revealed both the potential advantages of this technology and its challenges in this field (Qin, Hu, Qi & Chang, 2024). Their research affirms that even though Artificial Intelligence could greatly improve effectiveness and creativity in renewable power, it may have negative implications due to excessive use of power. This sophisticated comprehension of artificial intelligence's twofold effect on green energy provides key information about the wider consequences of AI integration, especially in terms of energy efficiency in smart cities.

In response to growing cyber threats, incorporating AI technologies into cybersecurity represents a significant advancement, particularly in smart cities (Ahmed et al., 2016). AI and machine learning (ML) technologies enhance cybersecurity by processing large volumes of data generated by IoT devices, identifying trends, and detecting anomalies that may indicate potential security breaches (Liu et al., 2018).

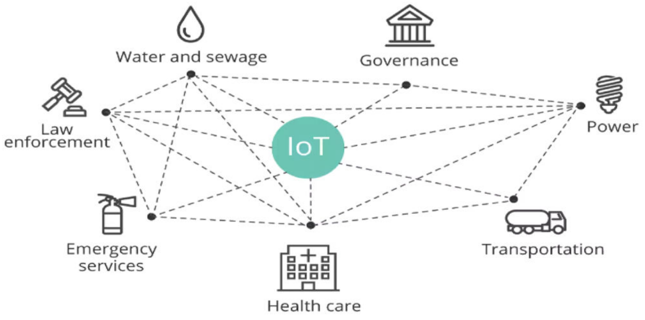

Fig. 3. Smart city IoT network.
Source: Pandey et al. (2019).

A critical application of AI in cybersecurity is anomaly detection, which identifies unusual patterns or behaviors that deviate from the norm. Real-time detection is crucial in smart cities, where IoT devices are continuously networked and exchanging data (Xu et al., 2014). AI/ML (Artificial Intelligence/ Machine Learning) models used in contemporary intrusion detection systems (IDSs) are capable of detecting anomaly-based attacks, though challenges such as balancing false positives and negatives for accurate threat detection remain Ali et al. (2022); Schmitt (2023).

However, despite AI's potential, its implementation in smart cities faces several challenges. These include the need for large, diverse, and high-quality datasets to train AI models (Liu et al., 2018). Additionally, adversarial AI attacks, where data is manipulated to deceive AI systems, require continuous updates and improvements to AI models (Guembe et al., 2022).

Ethical considerations in AI-driven smart city anomaly detection

Ethical considerations, particularly concerning privacy and surveillance, are also critical in the responsible deployment of AI in smart cities (Ahmad et al., 2022; Jing, Vasilakos, Wan, Lu & Qiu, 2014). The ethical dilemma regarding the application of AI in smart cities is also very important as it calls for careful attention to ensure responsible usage. Privacy and surveillance are major concerns because AI systems usually involve collecting and analyzing enormous amounts of personal data. When this happens, there may be an infringement on individual's privacy rights, turning into invasive surveillance practices. Therefore, public safety benefits from AI must be weighed against the need to protect individual's privacy (Ahmad et al., 2022).

Transparency and accountability in AI raises another concern. The complexity of AI algorithms, especially those using machine learning can make it difficult for stakeholders to understand how decisions are arrived at. Such opaqueness can hinder accountability more so when decisions made by artificial intelligence lead to unfavorable results. To maintain public trust, therefore, AI systems must be transparent with understandable decision-making processes (Jing et al., 2014).

In addition, some regulatory frameworks have been put in place to handle these ethical issues. For instance, under General Data Protection Regulation (GDPR), European Union ensures comprehensive regulation of data privacy and protection which demands that AI systems handling personal data within smart cities must prioritize privacy by default so as to conform to strict data protection laws (Badii, Bellini, Difino & Nesi, 2020). Other than GDPR, guidelines such as "Ethics Guidelines for Trustworthy AI" issued by European Commission include principles like fairness, transparency, and human oversight which are very appropriate for public-facing roles where ethics cannot be compromised (Weber, 2010).

Regulations at local and national levels significantly shape the use of AI in smart cities. These regulations often revolve around issues such as data sovereignty, cross-border data flows, and the ethical use of AI in public services (Floridi & Cowls, 2022). For example, some cities have created AI ethics boards to enforce local values and legal standards for the deployment of AI technologies (Whittaker et al., 2018). These boards and regulations ensure that AI systems are implemented in ways that respect local cultural norms and legal frameworks while addressing concerns about transparency and accountability (Barocas, Hardt & Narayanan, 2023).

In fact, ethical concerns and regulatory compliance are key to responsible deployment of AI technology in smart cities. In this context, adherence to frameworks like GDPR coupled with transparency, fairness and accountability as guiding principles, will enable smart cities to harness the potential of artificial intelligence so as to elevate quality while protecting rights of citizens and upholding trust from the public (Weber, 2010).

Human and policy aspects in smart city cybersecurity

Overcoming technological barriers is just one of the challenges facing effective adoption of AI-based cybersecurity solutions in smart cities. Among these are the ways people think, act, and trust such systems. To create trust between users, Shin (2021)) notes that transparency of AI systems is important. This becomes crucial especially when it comes to AI-driven cybersecurity where understanding how decisions are arrived at can greatly impact user acceptance and the effectiveness of these technologies.

Moreover, according to Davis (1989), AI-driven cybersecurity technologies in smart cities must be seen as effective, useful, and easy for end-users to operate. This perception directly influences their willingness to integrate AI solutions into their daily operations. Similarly, the role of attitudes, subjective norms, and perceived behavioral control (Ajzen, 1991) in shaping the adoption of AI in cybersecurity cannot be ignored. Therefore, if stakeholders feel that using artificial intelligence-enhanced security measures aligns with their values and is backed by their community or organization, they will likely adopt them.

Furthermore, Shin (2021)) investigated the ideas of explainability and causability, revealing that AI should be transparent and clear for end-users. The author emphasized that trust is established through transparency as acceptance and successful integration of AI technologies in smart city cybersecurity frameworks are improved. In this regard, users require awareness of the reasons behind choices made by AI systems, which is specifically vital in complex settings such as smart cities whereby cyber threats can cause far reaching damages. This will lead to greater trust between technology and its users in smart cities when AI systems provide explicit explanations for what they do.

Moreover, education, skills development, and awareness campaigns are important as well, in order to create a security-conscious culture that engages stakeholders in smart cities. Instead, as Malhotra, Srivastava and Gandotra (2019) argue, it is believed that these measures are necessary for educating people on ways of detecting cyber threats and dealing with them. By enhancing the cybersecurity literacy of residents, employees, and public officials, smart cities can build a more resilient defense against potential cyberattacks. According to Thakur (2024), ongoing training and education is pivotal considering the nature of continuously evolving digital threats; hence, all players must remain alert because new challenges will be addressed.

In conclusion, AI-based cybersecurity solutions in smart cities highly depend on human factors such as trust, attitudes and education, but this must always go hand in hand with user engagement efforts aimed at increasing their understanding. As a result, focus AI anomaly-based detection system designers should not only be inclined towards technological advancements but also on how these systems can successfully integrate into holistic urban ecosystems that finally support life within them through the active participation of the people they serve.

Conceptual model and propositions

Theoretical framework

This study's theoretical framework is based on a synergistic combination of multidisciplinary theories. These were carefully selected to thoroughly investigate how AI-enabled anomaly detection affects cybersecurity in the complex setting of smart cities.

To start with, the Theory of Complex Adaptive Systems (CAS) theory (Holland, 1995) – the main theory underpinning this study - offers a strong foundation for comprehending how different parts of smart city ecosystems interact dynamically, particularly with regard to cybersecurity. According to Holland (1995), as demonstrated in the "Complex Adaptive Systems" book, agents are the building blocks of complex adaptive systems, which are made up of pieces that interact with other agents to learn or adapt. All CAS have lever points, or places where a tiny directed movement results in massive, predictable changes in aggregate behavior. There are three levels of activity for all CAS agents: rule-discovery (creating new capabilities), credit-assignment (evaluating the use of existing capabilities), and performance (moment-by--moment capabilities). The adaptive interactions among its constituents always produce a CAS's behavior. These interactions also produce the hierarchical structure that distinguishes CASs—specific combinations of agents at one level become agents at the next higher level.

AI-enabled anomaly detection systems are a great fit for the idea of Complex Adaptive Systems (CAS), particularly when it comes to cybersecurity in smart cities. Let's examine the description given and discuss how AI systems work with anomaly detection.

CAS structure using adaptive agents

Agents in CAS adjust to each other based on their interactions (Walther, 2020). These agents, which are AI-enabled anomaly detection systems, can be thought of as standalone AI models or algorithms that are always learning and changing in response to fresh information and system interactions (Benbya, Nan, Tanriverdi & Yoo, 2020). For example, these agents, or AI models, in a smart city, adjust by picking up on new user behavior patterns, network traffic patterns, and possible security risks.

CAS lever points

Similar to how AI algorithms in anomaly detection can have a big influence, the notion of lever points in CAS describes how small directed actions can result in substantial changes in behavior (Grobman, 2005). The AI's ability to identify abnormalities can be significantly enhanced by minor adjustments to its settings or learning method. This is consistent with the idea of optimizing AI models for enhanced efficacy in detecting possible cyberthreats.

Three cas agent activity levels

The functions of AI systems in anomaly detection are correlated with the performance, rule-discovery, and credit-assignment levels of CAS agents (Fereidunian et al., 2015).

Performance: This refers to the day-to-day activities of the AI system, such as its ability to analyze network data in real-time and spot anomalies.

Credit Allocation: This can be thought of in terms of AI as the process of assessing and ranking how well various models or techniques identify security issues.

Rule-discovery is the process by which an artificial intelligence system learns or develops new algorithms or techniques to identify abnormalities, improving its capacity to counter new and unidentified cyberthreats.

Hierarchical structure and adaptive interactions

The behavior of the system in AI-enabled anomaly detection is the outcome of the adaptive interactions between different AI models and algorithms (Bii, Rimiru & Mwangi, 2022). These interactions result in creating a complex, tiered cybersecurity strategy guided by data and learning outcomes.

The way distinct AI models or layers function at different levels inside an anomaly detection system (Sarker, Furhad & Nowrozy, 2021) is similar to the hierarchical structure found in CAS. In order to create a multi-layered defense system, certain AI models may concentrate on preliminary data filtering and preprocessing, while others may concentrate on in-depth analysis or prediction (Garcia, Luengo & Herrera, 2015).

In conclusion, the CAS principles offer a framework for comprehending the behavior and evolution of AI-enabled anomaly detection systems, especially in intricate contexts like smart city networks. Advanced AI systems in the field of cybersecurity are characterized by their hierarchical system structure, adaptive learning, and agent (AI model) interaction. Based on the above discussion of Holland's CAS theory (Holland, 1995), the relevance of the CAS theory to this study is summarized in Table 2.

Three other theories prove essential to the holistic proposed model in our study. These are the TAM, or Technology Acceptance Model (Davis, 1989), Theory of Planned Behavior (Ajzen, 1991), and the Theory of Socio-Technical Systems (Emery & Trist, 1960). Davis's (1989) Technology Acceptance Model (TAM) describes how people adopt and utilize technology. It can be used to comprehend how AI-driven technologies are received and deployed in smart cities. Moreover, according to Ajzen's (1991) Theory of Planned Behavior (TPB), an individual's attitude toward a behavior, subjective standards, and perceived behavioral control influence their behavioral intentions, which drive behavior. Of course, TPB provides a structure for comprehending the intentional behavioral goals underlying the integration of AI in cybersecurity in smart cities. The decision to adopt AI-driven security measures is influenced by a number of factors, including attitudes, subjective norms, and perceived behavioral control. This idea emphasizes how crucial it is to match AI integration with the expectations and behavioral tendencies of different stakeholders in smart cities. Finally, according to the Theory of Socio-Technical Systems (Trist, 1981), organizational work systems are made up of social and technological components that need to work together in order for them to function properly. This theory emphasizes how social systems—such as the smart city environment and its residents—interact with technology in smart cities, specifically AI-driven anomaly detection. It highlights the necessity of designing and implementing AI systems in a way that not only considers technological specifications but also considers organizational, social, and cultural aspects of urban environments.

This study incorporates the above-mentioned theories to analyze the relationship between AI-driven anomaly detection and cybersecurity in smart cities. It is important to note that each of these frameworks offers a distinct perspective on this interaction. The field of CAS provides a holistic view of how AI and smart city components interact, focusing on their ability to adapt and learn. The Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB) specifically examine the psychological and social aspects that influence the acceptance and utilization of technology. These theories create a comprehensive framework that considers both the technology components of AI in smart cities and the influence of human behavior and organizational issues. This framework offers a more complete understanding of AI-driven cybersecurity.

Table 2
CAS Relevance in AI-enabled anomaly detection for enhanced cybersecurity in smart cities.

CAS Feature	Relevance to Study
CAS Structure Using Adaptive Agents	• Adaptive agents, or AI models and algorithms, make up CAS. • These agents interact with the system and data to learn and adapt. • Agents in anomaly detection adapt to novel threats and patterns.
CAS Lever Points	Modest CAS adjustments can have a big effect. Small changes to algorithms can significantly enhance anomaly detection in AI. AI models can be improved to identify cyber threats more accurately.
Three CAS Agent Activity Levels	Performance: AI systems' in-the-moment activities, such as network data analysis. Credit assignment: Assessing AI models' efficacy in threat identification. Rule-Discovery: creating fresh techniques to improve anomaly detection.
Hierarchical Structure and Adaptive Interactions	The adaptive interactions among AI models determine the behavior of the system. several models operating at different levels in a multi-layered AI method. AI structure that is hierarchical and has layers for analysis, prediction, and data processing

Integration of theories

The inclusion of CAS, TAM, and TPB in this paradigm is not random but rather crucial. CAS offers a high-level comprehension of the smart city as an intricate system in which AI-powered anomaly detection functions. The TAM (Technology Acceptance Model) and TPB (Theory of Planned Behavior) provide a detailed examination at the individual level, specifically looking at how humans interact with these devices. The framework illustrates the interdependence between technology and human elements by combining these different views. For example, CAS aids in comprehending the potential of AI systems to adapt within the smart city ecosystem, while TAM and TPB explain how human acceptance and behavioral goals directly impact the success of these systems in real-world applications. The integration ensures that the suggested model effectively tackles the technological and socio-technical aspects of AI-driven cybersecurity in smart cities.

Study propositions and conceptual model

AI-enabled anomaly detection and enhanced cybersecurity in smart city iot networks

Smart city environments with AI-enabled anomaly detection technologies are prime examples of complex adaptive systems in action (Ismail & Buyya, 2022), which aligns with the context of CAS framework. These technologies, which include a wide range of data analysis and machine learning capabilities, are dynamic by nature and are made to change and adapt to the ever-evolving threats and patterns in cybersecurity. Because of their adaptive nature, they are able to continuously improve their detection tactics, which is an essential ability considering how quickly cyber threats are changing (Schmitt, 2023; Ahmed et al., 2016). De facto, the ability of AI-driven anomaly detection to continuously adapt and learn from the IoT network (Liu et al., 2018) is what makes it effective in improving cybersecurity. The security and integrity of urban digital networks that are continually evolving and interconnected depend on this capability (Schmitt, 2023). These AI systems are essential for protecting smart cities from a wide range of cyberattacks since they are always learning to identify new patterns of risks (Ferrag et al., 2018).

Utilizing AI in cybersecurity arises as a tactical reaction to the complex and dynamic dangers present in Internet of Things networks, building on the adaptability of AI systems. Artificial intelligence (AI)-enabled solutions greatly improve the resilience and robustness of smart city cybersecurity infrastructures by continuously analyzing data and making adjustments in response to new information (Abdullahi et al., 2022; Ismail & Buyya, 2022). In addition to being reactive, this continuous process of adaptation and monitoring is proactive as well, seeing possible risks before they materialize as breaches (Schmitt, 2023; Xu et al., 2014).

Moreover, with a focus on zero-day threats, Ali et al. (2022) thoroughly analyze AI-based anomaly detection for cybersecurity. It emphasizes the necessity for cutting-edge AI techniques like deep learning and machine learning by highlighting the growth of cyber threats and the shortcomings of conventional security measures. In order to compare several methods for detecting zero-day attacks, the article addresses a variety of AI models, datasets, and evaluation criteria. It concludes that deep learning-based AI techniques are more successful at spotting and stopping complex cyberattacks, proving the beneficial correlation between improved cybersecurity and AI-based anomaly detection.

As a result, inside this intricate network of relationships, cybersecurity risks, IoT infrastructure, and AI systems are all integrated components rather than separate entities. The efficacy of artificial intelligence (AI) in augmenting cybersecurity is based on its capacity to maneuver and adjust inside this intricate system, reacting instantly to changing hazards. Thus, in light of this comprehensive analysis, the following proposition can be made:

> ***P1***: AI-enabled anomaly detection technologies are positively related to improved cybersecurity in the complex adaptive system of smart city IoT networks.

Role of human factors in the relationship between AI-enabled anomaly detection and enhanced cybersecurity in smart city IoT networks

The AI-powered solutions' efficacy aforementioned above isn't only based on how advanced their technology is. In this equation, the human aspect is a crucial factor. User perceptions, such as perceived ease of use and perceived usefulness, substantially impact the acceptance and effective use of technology (Ahmad et al., 2022). This conforms to TAM (Davis et al., 1989), and applies into how residents and city officials alike view and engage with AI-driven cybersecurity solutions in smart cities. The usefulness of AI-enabled anomaly detection in strengthening cybersecurity is vitally impacted by their engagement, confidence, and desire to employ these technologies.

In addition, by taking into account the impact of behavioral intentions, which are influenced by attitudes and subjective norms, as the Theory of Planned Behavior (TPB) (Ajzen, 1991) suggests, this effect will be even more clarified. The alignment of AI-enabled systems with human behavioral tendencies is necessary for these technologies to effectively improve cybersecurity (Chow et al., 2023). This alignment includes User-friendly interfaces, sufficient training, and awareness campaigns that improve comprehension and efficient application of AI technology in smart city ecosystems (Kitchin, 2014).

Consequently, human variables play a significant role in the effectiveness of AI-enabled anomaly detection systems in detecting and reducing cybersecurity threats. These comprise user attitudes, actions, and the general social and cultural preparedness to incorporate these technologies into day-to-day activities.

On the basis of this thorough comprehension, the following proposition can be put forth:

> ***P2***: In IoT networked smart city environments, human factors—such as user perceptions, behaviors, and social readiness to accept and efficiently utilize AI technologies—mediate the relationship between AI-enabled anomaly detection and enhanced cybersecurity.

Role of technological advancement and readiness in the relationship between AI-enabled anomaly detection and enhanced cybersecurity in smart city IoT networks

Although a clear and direct link exists between cybersecurity and AI-enabled anomaly detection, this relationship is not absolute or isolated. A number of moderating factors may have an impact, either strengthening or weakening it. This study emphasizes technological readiness as a main moderator impacting the AI-enabled anomaly detection – cybersecurity relationship. Furthermore, innovations in technology have a significant impact on how effective AI-powered anomaly detection systems are. These systems get more advanced with time, able to handle increasingly complex attacks and adjust to new cybersecurity difficulties (Yigitcanlar, Desouza, Butler & Roozkhosh, 2020). The degree of technical maturity can greatly impact how well AI technologies recognize and address cybersecurity threats and breaches in smart city settings (Liu et al., 2018). Therefore, the relationship between improved cybersecurity in smart cities and AI-enabled anomaly detection technologies is not linear; rather, it is driven by the dynamic interaction between AI-based technical improvements and technological readiness. The degree to which AI technologies may be successfully applied and incorporated into smart city cybersecurity infrastructure depends on these moderating elements.

This sophisticated comprehension allows for stating the following proposition:

> ***P3:*** Technological advancement moderates the relationship between AI-enabled anomaly detection and enhanced cybersecurity in IoT networked smart cities.

These factors collectively influence the efficacy and application of AI technologies in urban cybersecurity frameworks.

Based on the above discussion and derived propositions, the conceptual model of the study could be depicted as shown in Fig. 4.

Conceptual model constructs and dimensions

The main constructs of the model and their dimensions are discussed in the following sections.

A. ***AI-Driven Anomaly Detection Techniques***: These are the AI-driven approaches used to recognize and address cybersecurity risks (Hassan, Abrar, & Hasan, 2023) in IoT networks seen in smart cities (Caiazzo, Murino, Petrillo, Piccirillo & Santini, 2023). By modeling the actions that are deemed typical within a system and recognizing prospective assaults from behaviors that differ from the established normal behavior pattern, the anomaly-based approach seeks to discover new (unknown) attacks (Panagiotou, Mengidis, Tsikrika, Vrochidis & Kompatsiaris, 2021).
B. ***Cybersecurity Enhancement in Smart City IoT Networks***: this outcome variable measures how much smart city IoT networks' security and resistance to cyber threats have improved overall (Khatoun & Zeadally, 2017). The main indicators of enhanced IoT-networked smart city cybersecurity are social welfare, urban mobility solutions, operational resilience, and sustainability of the city. (Alahi et al., 2023). Of course, operational resilience is essential to ensure and maintain continuity in services and high uptime (Chakrabarty & Engels, 2020).
C. ***Human factors*** include user behavior, acceptance, and knowledge of cybersecurity measures driven by AI. The relationship between AI-driven anomaly detection and cybersecurity enhancing effectiveness is mediated by human variables, including: (Chow, Zhan, Wang & He, 2023; Adel, 2023; Ahmad et al., 2022; Cao, Duan, Edwards & Dwivedi, 2021)
   a. Acceptance and Adoption by Users: this dimension deals with how people accept and employ AI technologies, from citizens to municipal officials. It involves views of utility and simplicity of use, perceived performance expectancy, and perceived effort expectancy, which are crucial in determining the desire to interact with and use new technologies.
   b. Behavioral Intentions: this dimension examines how users' beliefs, subjective standards, and perceived behavioral control affect their intents and behaviors. It discusses how social forces and perceptions affect how AI technologies are used in smart cities.
   c. Training and Development of Skills: the degree of instruction and skill-building that AI system users can access. This aspect is essential for guaranteeing that people possess the skills and knowledge required to communicate with and operate AI-driven cybersecurity solutions. It also ensures that users are aware of possible dangers, follow safe procedures, and know how AI can help reduce the risk of cyberattacks.

Besides the dimensions mentioned above, two factors could be considered supporting components of human interaction with AI: perception of trust and reliability and social and cultural influences. To start with, trust is a key component influencing the intention to use and acceptability of AI solutions. This encompasses users' opinions of these technologies' reliability in identifying and countering cybersecurity risks and their faith in AI systems. The other factor, social and cultural influences, acknowledges the substantial influence that social settings and cultural norms can have on attitudes and behaviors regarding technology.

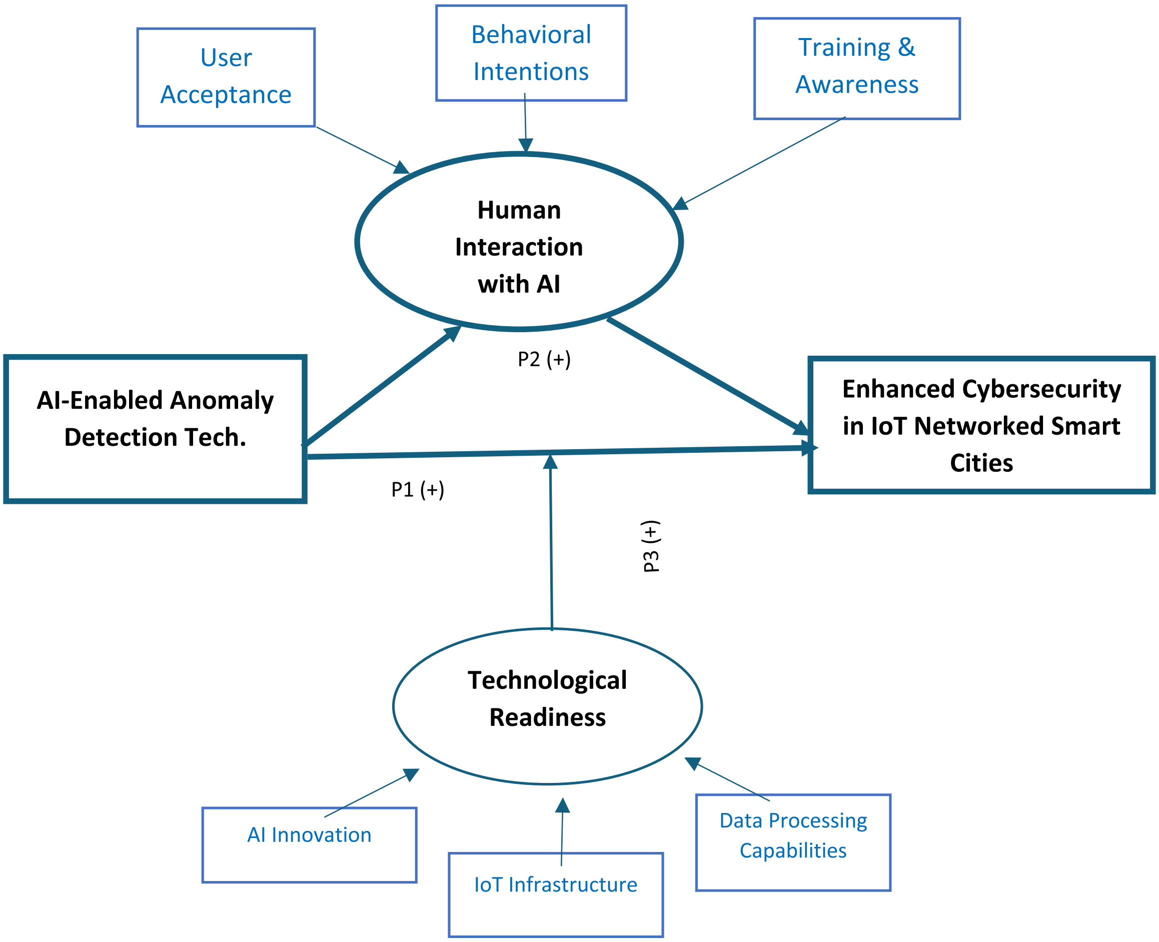
User Acceptance
Behavioral Intentions
Training & Awareness
Human Interaction with AI
P2 (+)
AI-Enabled Anomaly Detection Tech.
Enhanced Cybersecurity in IoT Networked Smart Cities
P1 (+)
P3 (+)
Technological Readiness
AI Innovation
IoT Infrastructure
Data Processing Capabilities

Fig. 4. Conceptual model and propositions.

D. Technological Readiness: technological advancements and readiness play a crucial role in shaping the efficacy of AI-enabled anomaly detection systems. As technology evolves, these systems become more sophisticated, capable of handling more complex threats and adapting to new cybersecurity challenges. The level of technological maturity can significantly influence how effectively AI tools identify and respond to threats in smart city environments. The concept of technology advancement could encompass: (Son et al., 2023; Alahi et al., 2023; Adel, 2023; Fatima, Desouza & Dawson, 2020; Liu et al., 2018):

a. Technological Innovation in AI and Machine Learning: this component deals with creating and applying novel machine learning and artificial intelligence algorithms. It covers innovations especially suited for cybersecurity applications in fields like deep learning, neural networks, and predictive analytics.
b. IoT Infrastructure Development: the degree of IoT infrastructure integration and sophistication in smart cities. This involves the implementation of sophisticated sensors, network systems, and connected devices that enable large-scale data gathering and exchange.
c. Capabilities for Data Analysis and Processing: the capacity to effectively handle and evaluate massive amounts of data produced by IoT networks in smart cities. This encompasses developments in edge computing, cloud computing, and big data technologies that improve the ability to manage and analyze large, complicated datasets.

Table 3
Mapping theories to framework components.

Framework Component	Complex Adaptive Systems (CAS)	Technology Acceptance Model (TAM)	Theory of Planned Behavior (TPB)
AI-driven Anomaly Detection Mechanism	Understanding the adaptability of AI systems within the smart city	Assessing user acceptance based on perceived usefulness	Evaluating behavioral intentions and attitudes towards AI systems
Human Interaction with AI Systems	Interaction between AI systems and human agents in smart cities	Perceived ease of use influencing AI adoption	Subjective norms and perceived behavioral control affecting AI use
Technological Integration in Smart Cities	Dynamic interactions between AI and other smart city elements	How perceived usefulness impacts broader technology acceptance	Social influence on the adoption of integrated technologies
Policy and Regulatory Implications	Utilizing CAS to understand the impact of regulations on AI behavior	Influence of regulations on perceived ease of use and usefulness	Impact of policy on subjective norms and perceived control

To better clarify the integration of the theoretical frameworks into the proposed AI-driven anomaly detection model, Table 3 maps each theory to the corresponding components of the conceptual model. This mapping illustrates how the adopted theories complement each other in explaining the different aspects of the model.

Moreover, the various theories underpinning each of the proposed relationships with justification of each are outlined in Table 4. The table illustrates how each theory is relevant to the specific relationships

Table 4
Theoretical validation of the model – relevance of theories to model relationships.

Theory	Relationship	Relevance & Justification
Complex Adaptive Systems (CAS) (Holland, 1995)	AI-enabled Anomaly Detection ➔ Enhanced Cybersecurity in Smart City IoT Networks	Smart city AI-powered anomaly detection systems can be thought of as adaptable agents inside these intricate networks. They constantly engage with and absorb large volumes of data, adapting to novel threat trends and risks. Understanding how AI technologies dynamically enhance the security and resilience of smart cities requires this viewpoint.
Technology Acceptance Model (TAM) (Davis, 1989) **Theory of Planned Behavior** (Ajzen, 1991)	AI-enabled Anomaly Detection ➔ Human Factor ➔ Enhanced Cybersecurity in Smart City IoT Networks	• The usefulness and usability of AI-driven anomaly detection are seen differently by different stakeholders in smart cities, and this perception affects their acceptance and support for such technologies. TAM can be used to examine this perception. • By examining how people's attitudes, social norms, and control perceptions affect how AI is implemented and used in cybersecurity, this theory can assist in better understanding the human interaction with AI in the framework.
Theory of Socio-Technical Systems (Emery & Trist, 1960)	AI-enabled Anomaly Detection * [Technological, Policy, and Environmental Factors] ➔ Enhanced Cybersecurity in Smart City IoT Networks	Blending social and technical factors is especially relevant to comprehend how AI-driven anomaly detection is integrated into smart cities, striking a balance between technological efficiency and social considerations like user trust and legal compliance.

within the proposed framework. This helps to support the theoretical grounding of the model and its components.

Discussion

Drawing on a solid theoretical framework, this study proposed a multi-lens model that added to the body of literature emphasizing that integrating AI-enabled anomaly detection into smart city IoT networks significantly improves cybersecurity (e.g., Villegas-Ch, Govea & Jaramillo-Alcazar, 2023; Jia et al., 2023; Ullah, Al-Turjman, Mostarda & Gagliardi, 2020). The Complex Adaptive Systems (CAS) theory, which forms the basis of this study's model, offers a thorough foundation for comprehending this integration. According to research by Liu et al. (2018) and Ahmed et al. (2016), the capacity of AI-enabled systems for adaptation and learning is essential for mitigating the ever-changing nature of cyber threats. The model also highlights how important human aspects and social and environmental factors are to AI technologies' efficacy, which is consistent with the ideas of the Theory of Planned Behavior (TPB) (Ajzen, 1991), the Technology Acceptance Model (TAM) (Davis, 1989), and the Socio-Technical Systems Theory (Emery & Trist, 1960).

In this study, the examination of AI-enabled anomaly detection in smart city IoT networks sheds light on an entangled but interesting relationship between human interaction with AI and technological readiness. The proposed model gives us a holistic view of the cybersecurity landscape in smart cities because it is grounded on a multi-lens approach. It points out how both technology readiness and human interaction with AI strongly influence cybersecurity.

AI-enabled anomaly detection stands out as one of the leading paradigms in this area that represent a crucial leap in technology for making our cyberspace safe. In accordance with Ahmed et al. (2016) and Liu et al. (2018), our model underscores the significance of adaptability and learning capability that helps AI systems tackle constantly growing security threats connected with deployment of smart city services at all times. These are adaptive systems, directed by advanced algorithms, which can change their behavior to deal with new threats instead of being static entities—a feature resonant with Complex Adaptive Systems (CAS) theory. This is particularly significant given the complicated nature of IoT devices underpinning smart cities.

Our model, shifting from technology to human role underscores the fact that success of AI-enabled anomaly detection in the conventional cyber security techniques often overlooks key human variables. It is, therefore, peoples' perceptions concerning its usefulness and ease of use that will determine whether AI systems for smart cities are acceptable and effectively used. Additionally, by broadening this concept into cyber security, our model argues that AI systems must be not only technologically advanced but also tailored towards the preferences and behavioral patterns of their end users for them to function effectively. Similarly, this model acknowledges diverse stakeholder's capabilities necessitating skills enhancement through appropriate and continuous training and knowledge updating via awareness campaigns.

Moreover, the effect of the regulatory and policy environment, although not part of the proposed model, still remains a supporting element, especially when it comes to AI-driven cybersecurity in smart cities. In addition, Weber (2010) and Roman et al. (2013) underline that regulation is integral in ensuring AI technologies do not cross ethical and legal limits. These frameworks describe the demands for safety protocols, privacy policies, and general governance of AI technology. Consequently, they determine how cyber security measures are put into practice. Moreover, the regulatory framework and policies also play a crucial role in this relationship. The capabilities of AI systems in cybersecurity applications can be either enabled or restricted by laws and policies pertaining to data privacy, security requirements, and the use of AI technology. AI-enabled systems can have a more significant impact on cybersecurity if effective legislative frameworks are in place to encourage innovation while maintaining security and privacy (Chakrabarty & Engels, 2020). On the other hand, outmoded or restrictive policies could limit their potential (Weber, 2010; Roman et al., 2013).

The main point in this model is that it acknowledges human-technology interaction as crucial in anomaly detection enabled by AI. At the same time, however, such technologies are framed within regulatory landscapes which impact their effectiveness (Weber, 2010). Such policies include regulations requiring constant updates on artificial intelligence systems to ensure compliance with data privacy principles, thereby fostering a robust operational environment for AI solutions. Moreover, Weber (2010) work has revealed that there are also some provisions for ethics within these regulatory frameworks to check on misuse of AI; hence building trust among the public towards any smart city contexts.

Moreover, the proposed conceptual framework offers important insights that can form the basis for policy frameworks aimed at facilitating effective deployment of AI-enabled cybersecurity systems in smart cities. One major policy implication is the necessity for creating flexible yet robust regulatory frameworks capable of adapting to changing AI technology dynamics. To ensure continued learning and adaptation by AI systems, policies must facilitate their periodic updates so that ethical considerations regarding citizen privacy and data security are upheld.

Additionally, the model points out that AI deployment must be in line with wider socio-technical systems. In other words, policy interventions should not only focus on technological advancements but also consider human and organizational forces influencing the effectiveness of AI towards enhancing cybersecurity. An example of which is policies focused on continuous professional development as well as training for managers dealing with AI systems that would improve the human aspect of cybersecurity; thus ensuring that AI technologies are used and maintained properly.

This theoretical framework contributes to an ongoing conversation by blending what are often separate discussions around technology, human behavior, and regulatory environments. It calls for a more holistic approach to cyber security in smart cities where these dimensions are considered interconnected and mutually reinforcing. This theoretical contribution stands against traditional siloed approaches and provides a more integrated view that can be used as a basis for future research and practical policy-making.

Although our model corroborates with the extant literature regarding the impact of AI-based anomaly detection on enhanced smart city cybersecurity, it differs from previous research in that it is holistic and tri-lens. The model incorporates all relevant factors that impact cybersecurity in smart cities. Although prior research has frequently concentrated on discrete features like technology capabilities (Liu et al., 2018) or policy consequences (Weber, 2010), our model integrates these components with the occasionally disregarded issue of human factors. This all-encompassing strategy fills in a knowledge gap on the ways in which different elements interact and affect AI's effectiveness in cybersecurity.

To sum up, this work adds a great deal to the extant body of information by providing a model that both complements and advances the existing literature. With the integration of human elements and technology readiness, and supported by a relevant regulatory framework, the model provides a more nuanced and comprehensive view of cybersecurity in smart city IoT networks. It emphasizes the significance of a well-rounded strategy that takes into account the technical aptitude of AI systems, the perceptual and behavioral characteristics of users, and the directing impact of legal and regulatory frameworks. This model emphasizes the necessity for various tactics in addressing the intricate difficulties of cybersecurity in smart cities and serves as a blueprint for future study and practice.

Implementation roadmap

A roadmap followed diligently through best practices adopted by different cities is mission-critical to implement AI-driven anomaly detection systems which enhance cyber security leading to improved safety in urban areas. This section outlines a path to translate the conceptual framework into practical strategies for practitioners.

Adopting AI-driven anomaly detection in smart cities begins with a comprehensive assessment of existing infrastructure (Kalinin, Krundyshev & Zegzhda, 2021), including IoT networks, data management systems, and cybersecurity measures. This evaluation identifies gaps that need enhancement for effective AI integration. It is crucial to engage stakeholders, such as city officials, IT professionals, and cybersecurity experts (Xia, Semirumi & Rezaei, 2023) to align objectives, allocate resources, and address public concerns about privacy and data security.

Following this assessment, cities should select appropriate AI tools and technologies based on factors like scalability, system compatibility, and real-time data processing capabilities (Usurelu & Pop, 2017). Both open-source and commercial solutions should be considered to find the best fit for the city's needs. Pilot testing in controlled environments is recommended to evaluate system performance, identify challenges, and make necessary adjustments. Monitoring key metrics, such as detection accuracy and system responsiveness, is essential during this phase (Thakkar & Lohiya, 2022).

The AI-driven anomaly detection system can be integrated into the city's broader cybersecurity framework upon successful pilot tests. This involves deploying AI models across IoT networks and establishing real-time monitoring systems (Villegas-Ch, Garcia-Ortiz & Sánchez-Viteri, 2024). Continuous monitoring post-deployment is critical to ensure the system adapts to emerging threats (Ginart, Zhang & Zou, 2022). Regular updates and refinements of AI-enabled models will help maintain system accuracy and effectiveness. To enable successful adoption, robust data governance frameworks that prioritize data privacy and security are necessary and in line with regulations such as the General Data Protection Regulation (GDPR). An AI system that will grow with increasing IoT networks and data sources should also be scalable (Manihar, Bano, Patel, & Agrawal, 2020). City personnel must be trained, providing them with the necessary skills to handle AI-enabled systems as well as how to detect any anomalies (Alahi et al., 2023).

Incorporating ethical considerations like transparency, accountability and bias are very important during the deployment process. Promoting ethical AI practices will help develop public trust (Knowles & Richards, 2021). To utilize the latest advancements and ensure success in the implementation process, it is recommended they collaborate with tech partners and professionals (Brock & Von Wangenheim, 2019).

Implications and future research recommendations

This study has significant implications for both the theoretical and practical areas of cybersecurity in smart cities. First, the proposed conceptual framework adds to existing literature by having several theories such as Complex Adaptive Systems (CAS) theory, Technology Acceptance Model (TAM), and Theory of Planned Behavior (TPB) all together. This method provides a deep understanding of how AI-driven technologies collaborate with human and technology factors to enhance cyber security. Consequently, it explores how future research can cope with the various dimensions related to cyber security in smart cities.

From a practical standpoint, this study suggests that human elements and technological readiness should be considered when deploying AI-based cyber-security solutions. In summary, policy makers, city planners along with IT experts must not only consider the technical prowess of these systems but also their ability to align with user needs and behavior patterns. On balance, this article calls for the development of AI systems that prioritize transparency and user-centeredness to facilitate widespread acceptance and seamless integration into urban landscapes.

Future research should concentrate on experimentally examining the suggested conceptual framework. This study has provided a theoretical foundation; however, there is a need to discern AI-enabled anomaly detection, human interaction with AI, and technological readiness in real-world smart city environments. Data could be collected through surveys, case studies, and field experiments to examine the model's propositions. Moreover, further studies may delve into issues such as privacy, surveillance, or even possible biases in-built within AI algorithms. Understanding these aspects will help in creating AI systems that are not only effective, but also ethical and socially responsible. Future research could be helpful in understanding the long-term implications of human factors in AI-driven technology adoption by using longitudinal studies that trace shifts in user perceptions, attitudes, and behaviors over time. Thus, this would enable a realization of how continuous training, awareness programs and changing technologies affect the efficacy of cybersecurity measures within smart cities.

Lastly, cross-cultural research is needed to examine how different cultural contexts influence the adoption and effectiveness of AI-driven cybersecurity technologies. Such comparative studies among smart cities across regions and cultures will enable future work to identify best practices while tailoring AI systems to meet unique needs based on different populations.

As we stand at the nexus of urban evolution and technology change, this study envisions a future where our digital and urban domains are protected with unparalleled accuracy and foresight by tying together the threads of AI-enabled anomaly detection, human-centric design, and dynamic policy landscapes. Our model serves as more than just a roadmap for this trip; it is a lighthouse that points the way to a safer, smarter, and more secure urban future.

CRediT authorship contribution statement

Heng Zeng: Writing – original draft, Methodology, Investigation, Conceptualization. **Manal Yunis:** Writing – original draft, Visualization, Resources, Project administration, Methodology, Investigation, Conceptualization. **Ayman Khalil:** Writing – original draft, Visualization, Validation, Methodology, Investigation, Conceptualization. **Nawazish Mirza:** Writing – original draft, Conceptualization.

References

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics, 11*(2), 198.

Adel, A. (2023). Unlocking the future: Fostering human–machine collaboration and driving intelligent automation through industry 5.0 in smart cities. *Smart Cities, 6*(5), 2742–2782.

Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review, 43*, Article 100452.

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19–31.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179–211.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.

Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends. *Sensors, 23*(11), 5206.

Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. I. (2022). Comparative evaluation of AI-based techniques for Zero-Day attacks detection. *Electronics, 11*(23), 3934.

Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies, 33*(3), e3677.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., & Lever, C. (2017). Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)* (pp. 1093–1110).

Ashraf, Q. M., Tahir, M., Habaebi, M. H., & Isoaho, J. (2023). Toward autonomic internet of things: Recent advances, evaluation criteria, and future research directions. *IEEE Internet of Things Journal, 10*(16), 14725–14748.

Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE access : practical innovations, open solutions, 8*, 23601–23623.

Barocas, S., Hardt, M., & Narayanan, A. (2023). *Fairness and machine learning: Limitations and opportunities*. Cambridge, MA: MIT Press.

Benbya, H., Nan, N., Tanriverdi, H., & Yoo, Y. (2020). Complexity and information systems research in the emerging digital world. *MIS quarterly, 44*(1), 1–17.

Bii, J. K., Rimiru, R., & Mwangi, R. W. (2022). OAAE: Optimized adaptive anomaly detection ensemble—Base model boosting by parameter optimization. *Engineering Reports, 4*(2), e12449.

Blake, A. (2018). Malware infection poised to cost $1 million to Allentown (February 21, 2018). Retrieved from.

Brock, J. K. U., & Von Wangenheim, F. (2019). Demystifying AI: What digital transformation leaders can teach you about realistic artificial intelligence. *California management review, 61*(4), 110–134.

Caiazzo, B., Murino, T., Petrillo, A., Piccirillo, G., & Santini, S. (2023). An IoT-based and cloud-assisted AI-driven monitoring platform for smart manufacturing: Design architecture and experimental validation. *Journal of Manufacturing Technology Management, 34*(4), 507–534.

Cao, G., Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2021). Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision-making. *Technovation, 106*, Article 102312.

Chakrabarty, S., & Engels, D. W. (2020). Secure smart cities framework using IoT and AI. In *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)* (pp. 1–6). IEEE.

Chow, C. S. K., Zhan, G., Wang, H., & He, M. (2023). Artificial Intelligence (Ai) Adoption: An extended compensatory level of acceptance. *Journal of Electronic Commerce Research, 24*(1), 84–106.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—A survey. *Electronics, 12*(8), 1920.

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Applied Sciences, 13*(2), 790.

Ejaz, W., & Anpalagan, A. (2019). Internet of Things for Smart Cities: Overview and Key ChallengesW. Ejaz, & A. Anpalagan (Eds.). *Internet of Things for Smart Cities: Technologies, Big Data and Security*, 1–15. https://doi.org/10.1007/978-3-319-95037-2_1. Springer International Publishing.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research, 5*(4), 491–497.

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. *Management Science, Models and Techniques, 2*, 83–97.

Fatima, S., Desouza, K. C., & Dawson, G. S. (2020). National strategic artificial intelligence plans: A multi-dimensional analysis. *Economic Analysis and Policy, 67*, 178–194.

Fereidunian, A., Lesani, H., Zamani, M. A., Kolarijani, M. A. S., Hassanpour, N., & Mansouri, S. S. (2015). A complex adaptive system of systems approach to human–automation interaction in smart grid. *Contemporary issues in systems science and engineering*, 425–500. https://doi.org/10.1002/9781119036821.ch12. John Wiley & Sons, Ltd.

... Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., Janicke, H., & Raza, I. (2018). Blockchain technologies for the Internet of Things: Research issues and challenges *IEEE Internet of Things Journal, 6*(2), 2188–2204

Floridi, L., & Cowls, J. (2022). A unified framework of five principles for AI in society. *Machine learning and the city* (pp. 535–545). John Wiley & Sons, Ltd.. https://doi.org/10.1002/9781119815075.ch45

Garcia, S., Luengo, J., & Herrera, F. (2015). *Data preprocessing in data mining, 72* pp. 59–139). Cham, Switzerland: Springer International Publishing.

Ginart, T., Zhang, M. J., & Zou, J. (2022). Mldemon: Deployment monitoring for machine learning systems. In *International conference on artificial intelligence and statistics* (pp. 3962–3997). PMLR.

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1294–1312.

Grobman, G. (2005). Complexity theory: A new way to look at organizational change. *Public Administration Quarterly, 29*(3), 351–384.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence, 36*(1), Article 2037254.

... Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., & Chiroma, H. (2016). The role of big data in smart city *International Journal of Information Management, 36*(5), 748–758

Hassan, M. M., Abrar, M. F., & Hasan, M. (2023). An explainable AI-driven machine learning framework for cybersecurity anomaly detection. *Cyber security and business intelligence*. Routledge. https://doi.org/10.4324/9781003285854

Holland, J. H. (1995). *Hidden order. Business Week-Domestic* (Edition, p. 21). https://www.academia.edu/download/95656325/_Helix_Books_John_Holland_Hidden_Order_How_Adaptation_Builds_Complexity_Helix_Books_Basic_Books_1996_.pdf.

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: Insights from industry surveys. *The Journal of Risk Finance, 22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Huber, B., Kandah, F., & Skjellum, A. (2023). BEAST: Behavior as a service for trust management in IoT devices. *Future Generation Computer Systems, 144*, 165–178.

Ismail, L., & Buyya, R. (2022). Artificial intelligence applications and self-learning 6G networks for smart cities digital ecosystems: Taxonomy, challenges, and future directions. *Sensors, 22*(15), 5750.

Jia, Y., Gu, Z., Du, L., Long, Y., Wang, Y., Li, J., et al. (2023). Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. *Knowledge-Based Systems, 276*, Article 110781.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines, 9*(4), 78.

Kaspersky (2023). Kaspersky unveils an overview of IoT-related threats in 2023 (September). Retrieved from https://www.kaspersky.com/about/press-releases/2023_kaspersky-unveils-an-overview-of-iot-related-threats-in-2023.

C. Cyrus, "IoT Cyberattacks Escalate in 2021, According to Kaspersky," 17 2021. [Online]. Available: https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine, 55*(3), 51–59.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1–14.

Knowles, B., & Richards, J. T. (2021). The sanction of authority: Promoting public trust in AI. In *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency* (pp. 262–271).

Konstantopoulou, E., Sklavos, N., & Ognjanovic, I. (2023). Securing public safety mission-critical 5G communications of smart cities. *Internet of everything for smart city and smart healthcare applications* (pp. 61–74). Cham: Springer Nature Switzerland.

Linde, L., Sjödin, D., Parida, V., & Wincent, J. (2021). Dynamic capabilities for ecosystem orchestration A capability-based framework for smart city innovation initiatives. *Technological Forecasting and Social Change, 166*, Article 120614.

Liu, F., Su, C. W., Tao, R., Qin, M., & Umar, M. (2024). Fintech and aluminium: Strategic enablers of climate change mitigation and sustainable mineral policy. *Resources Policy, 91*, Article 104934. https://doi.org/10.1016/j.resourpol.2024.104934

Liu, Y., Zhang, P., & Zhou, J. (2018). Using AI to enhance the security of Internet of Things. *Sensors, 18*(2), 403.

Lu, Y., Xu, L. D., & Xu, J. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal, 6*(2), 2103–2115.

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports, 7*, 7999–8012.

Malhotra, C., Srivastava, A., & Gandotra, V. (2019). Cybersecurity and smart cities: Establishing the need for capacity building. *Cybernomics, 1*(3), 6–15.

Makpotche, M., Bouslah, K., & M'Zali, B. (2024). Corporate governance and green innovation: International evidence. *Review of Accounting and Finance, 23*(2), 280–309. https://doi.org/10.1108/RAF-04-2023-0137

Manihar, S., Bano, T., Patel, R., & Agrawal, S. (2020). Intelligent and scalable IoT Edge-cloud system. *International Journal of Advanced Computer Science and Applications, 11* (8). https://doi.org/10.14569/IJACSA.2020.0110846

Mehta, P., Pandit, A. K., & Modi, C. (2020). Machine learning-based anomaly detection techniques for smart cities: A survey. *Information Processing & Management, 57*(3), Article 102181.

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in smart city initiatives: Some stylised facts. *Cities (London, England), 38*, 25–36.

Panagiotou, P., Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Host-based intrusion detection using signature-based and ai-driven anomaly detection methods. *Information & Security, 50*(1), 37–48.

Pandey, P., Golden, D., Peasley, S., & Kelkar, M. (2019). Making smart cities cybersecure. Retrieved from https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html.

Qin, M., Hu, W., Qi, X., & Chang, T. (2024). Do the benefits outweigh the disadvantages? Exploring the role of artificial intelligence in renewable energy. *Energy Economics, 131*, Article 107403.

Rehan, H. (2023). Internet of Things (IoT) in smart cities: Enhancing urban living through technology. *Journal of Engineering and Technology, 5*(1), 1–16.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks, 57*(10), 2266–2279.

Rangu, C. M., Badea, L., Scheau, M. C., Gǎbudeanu, L., Panait, I., & Radu, V. (2024). Cyber insurance risk analysis framework considerations. *The Journal of Risk Finance, 25*(2), 224–252. https://doi.org/10.1108/JRF-10-2023-0245

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science, 2*(3), 173.

Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration, 36*, Article 100520.

Shahidehpour, M., Li, Z., & Ganji, M. (2018). Smart cities for a sustainable urbanization: Illuminating the need for establishing smart urban infrastructures. *IEEE Electrification magazine, 6*(2), 16–33.

Sharma, A., & Jain, P. (2023). Adaptability of IoT and cloud for enabling the smart city: Applications and challenges. *Handbook of research on network-enabled iot applications for smart city services* (pp. 54–74). IGI Global. https://doi.org/10.4018/979-8-3693-0744-1.ch004

Sharma, H., Haque, A., & Blaabjerg, F. (2021). Machine learning in wireless sensor networks for smart cities: A survey. *Electronics, 10*(9), 1012.

Shehadeh, M., Hussainey, K., Alhadab, M., & Kilani, Q. (2024). Corporate narrative reporting on Industry 4.0 technologies: Do the COVID-19 pandemic and governance structure matter? *Review of Accounting and Finance, 23*(5), 687–714.

Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies, 146*, Article 102551.

Shu, H., Wang, Y., Umar, M., & Zhong, Y. (2023). Dynamics of renewable energy research, investment in EnvoTech and environmental quality in the context of G7 countries. *Energy Economics, 120*, Article 106582. https://doi.org/10.1016/j.eneco.2023.106582

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.

Singh, A.P. (.2023). AI in Cyber Security: Advantages, Applications and Use Cases. Retrieved from https://www.analyticsvidhya.com/blog/2023/02/future-of-ai-and-machine-learning-in-cybersecurity/.

Son, T. H., Weedon, Z., Yigitcanlar, T., Sanchez, T., Corchado, J. M., & Mehmood, R. (2023). Algorithmic urban planning for smart and sustainable development: Systematic review of the literature. *Sustainable Cities and Society, 94*, Article 104562.

Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review, 55*(1), 453–563.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE), 4*(1), 1–20.

Trist, E. L. (1981). *The evolution of socio-technical systems (Vol. 2)*. Toronto: Ontario Quality of Working Life Centre.

Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. *Computer Communications, 154*, 313–323.

Umair, M., Cheema, M. A., Cheema, O., Li, H., & Lu, H. (2021). Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT. *Sensors, 21*(11), 3838.

Usurelu, C.-C., & Pop, C. (2017). My city dashboard: real-time data processing platform for smart cities. *Journal of Telecommunications and Information Technology, 1*. http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-494697bf-494c-4c9c-925c-8f5cd7773ef6.

Vailshery, L. S. (2023). *Number of internet of things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030*. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide.

Villegas-Ch, W., Govea, J., & Jaramillo-Alcazar, A. (2023). IoT Anomaly detection to strengthen cybersecurity in the critical infrastructure of smart cities. *Applied Sciences, 13*(19), 10977.

Villegas-Ch, W. E., Garcia-Ortiz, J. V., & Sánchez-Viteri, S. (2024). Toward intelligent monitoring in IoT: AI applications for real-time analysis and prediction. *IEEE access : practical innovations, open solutions, 12*, 40368–40386.

Walther, A. (2020). From responsive to adaptive and interactive materials and materials systems: A roadmap. *Advanced Materials, 32*(20), Article 1905111.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30.

... Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., & Schwartz, O. (2018). *AI now report 2018* (pp. 1–62). New York: AI Now Institute at New York University

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. *IEEE access : practical innovations, open solutions, 8*, 153826–153848.

Xia, L., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society, 98*, Article 104771.

Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

Yigitcanlar, T., Desouza, K. C., Butler, L., & Roozkhosh, F. (2020). Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies, 13*(6), 1473.

Zhang, Y., Deng, R. H., Liu, X., Zheng, D., & Mahmood, A. (2019). Analysis and outlook: From network security to cybersecurity. *Journal of Computer Research and Development, 56*(1), 1–21.