**Cyber Forensics Analysis of Honeypot for Threat Detection in Smart Cities**

Sathyendraa A/L Karmukilan1, a), Mohammad Shadab Khan1, 2, b) and Syed Qamrun Nisa1, 3, c)

*1Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia.*

*2Centre of Advanced Analytics, COE for Artificial Intelligence, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia.*

*3Centre for Image and Vision Computing (CIVC), COE for Artificial Intelligence, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia.*

*c)Corresponding author: qamrunnisa@mmu.edu.my*

*a) 1211104919@student.mmu.edu.my*

*b) shadab.khan@mmu.edu.my*

**Abstract.** Smart cities increasingly rely on Internet of Things (IoT) technologies to enhance urban living through interconnected systems supporting transportation, governance, energy, and healthcare. While these advancements bring efficiency and sustainability, they also introduce complex cybersecurity vulnerabilities. This paper presents a literature-based analysis of smart city architectures and common cyber threats such as DDoS attacks, brute-force in- trusions and port scanning. To address these challenges, we explore the role of honeypots—simulated environments designed to detect, prevent, and analyze malicious activities. The study categorizes honeypots into different types of interaction models, highlighting their trade-offs in realism, resource consumption, and attacker engagement. They demonstrate varied effectiveness in capturing adversarial behavior. Focus is given to Secure Shell (SSH) services, a frequent target of brute-force attacks, with honeypot data revealing significant probing activity from specific geograph- ical regions. The findings support the strategic use of honeypots in smart city infrastructure to improve threat detection, gather actionable intelligence, and mitigate risks. The paper concludes by recommending the integration of honeypot- based monitoring into existing cybersecurity frameworks as a cost-effective measure for enhancing resilience in smart city networks.

# INTRODUCTION

A Smart City is a digitally advanced urban area enabled by technologies like the Internet of Things (IoT) [1]. This innovative use of IoT employs a variety of electronic techniques to collect data and combine the various layers of a city’s infrastructure, allowing for strategic decision-making and data collection in areas like climate control and transportation [2].

Many nations’ governments successfully use these technologies to improve urban systems, integrating innovations such as sensors for ambient conditions and pedestrian movement to increase the effectiveness and usefulness of city services [3].

Normal cities are actively transforming into smart cities. For example, the nation of Saudi Arabia has allocated 5 billion USD for the development of NEOM, which represents an innovative smart city project [4]. Through its ITS system, Riyadh monitors traffic using adaptive control along with sensors and modern CCTV technology to mitigate congestion in the city [4].

The storage and collection of sensitive urban data create substantial privacy concerns that make cities vulnerable to cybercriminal activity [1]. In addition to ransomware and malware contamination, smart cities also face distributed denial-of-service (DDoS) attacks and internal threats that affect critical infrastructure components, IoT devices, com- munication networks, and sensitive data storage facilities [2]. Shielding sensitive data requires the implementation of modern strategic methods, since these threats are constantly evolving [3].

The integration of different IoT devices in urban frameworks has generated a complex security landscape that introduces multiple threats due to the adoption of new technologies in smart city development [5]. The absence of established security protocols within smart city systems further exposes them to cyberattacks [1]. Honeypots are security solutions that use virtual versions of vulnerable targets to deceive attackers and gather important information about their tactics, including attack strategies, tools, and techniques [6]. Through the development of robust security strategies, the knowledge gathered enables organisations to enhance their overall security posture [6].

# LITERATURE REVIEW

## Smart Cities

The Internet of Things (IoT) plays a foundational role in smart city infrastructure by facilitating an interconnected network of physical devices that communicate and transmit data via the internet [7]. Smart cities leverage IoT-enabled technologies such as sensors, actuators, and cameras for applications including energy management, waste collection, and traffic regulation [2]. However, the heterogeneity of IoT devices and communication protocols, often compounded by weak or hardcoded passwords, introduces significant security vulnerabilities to smart city networks [7].

Smart city services are structured through a multilayered architecture. The foundational technological layer in corporates advanced and widely adopted technologies to address urban challenges such as energy efficiency, trans- portation, and public safety [1]. Above this is the network communication layer, which ensures interoperability and seamless connectivity among devices and systems [1]. This layered framework underpins diverse service domains including smart transportation, smart communities, and smart environments aimed at enhancing urban sustainability and residents’ quality of life [1].

Smart transportation systems in smart cities enhance mobility by providing optimal route guidance, enabling car and bike-sharing services, and improving the efficiency of public transportation [1]. Singapore exemplifies this approach with its strategic initiatives that reduce traffic congestion and promote sustainable transport, particularly through its well-integrated Mass Rapid Transit (MRT) system [8]. Smart community leverages information and communication technologies (ICT) to empower individuals, institutions, and geographic regions [1]. It is generally categorized into smart economy and smart governance, relying on broadband infrastructure to facilitate innovation in commerce, education, healthcare, and governance services [9]. Notable implementations include Amsterdam Smart City, which fosters collaboration among businesses, government, and citizens to address urban challenges in domains such as living and mobility [10].

Smart living integrates real-time information sharing to help citizens address everyday challenges and stay con- nected [1]. It includes domains such as smart healthcare, smart people, smart education, and smart homes. Smart healthcare improves diagnostics and treatment through interconnected devices that stream patients’ vital signs [11]. The concept of smart people emphasizes high Human Development Index (HDI), lifelong learning, diversity, and adaptability [12]. Smart education offers digital tools and online delivery systems to facilitate modern learning en- vironments [13]. In smart homes, automation systems controlled via smartphones or tablets allow users to manage appliances like lights, fans, air conditioners, and security locks using Bluetooth or Wi-Fi [11]. Smart environments enable real-time monitoring and autonomous management of systems such as smart buildings, factories, and energy infrastructure to enhance efficiency and sustainability [1]. These ecosystems operate continuously to provide ser- vices that promote energy conservation, environmental protection, and community engagement even during economic downturns [12]. Smart factories, driven by advanced technologies, are crucial for innovation in manufacturing [5]. Smart buildings use ICT to optimize operations and reduce energy consumption by integrating various building sys- tems [14]. Additionally, home energy management systems allow consumers to monitor and adjust appliance usage, although automation for direct control remains limited. Evaluations of Energy Management Systems (EMS) consider metrics such as power usage and temperature data pre- and post-installation [15]. Summary of smart city applications and outcomes is tabulated in Table 1.

## Common Attacks in Smart Cities

The Mirai botnet is a form of malware targeting Internet of Things (IoT) devices, converting them into bots for executing large-scale distributed denial-of-service (DDoS) attacks [16]. It first gained notoriety in mid-September 2016 with massive attacks on sites such as Krebs on Security, OVH, and Dyn, crippling services like Amazon, Netflix, and PayPal through a 1.2 Tbps attack involving approximately 100,000 IoT devices [16]. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are disruptive cyber activities that aim to render systems or networks inaccessible [17]. While DoS attacks originate from a single source, DDoS attacks utilize multiple distributed agents, so the attack lifecycle typically includes identifying and exploiting vulnerabilities to infect systems and expanding the botnet through automated means [17, 18].

**TABLE 1.** Summary of smart city applications and outcomes

|  |  |  |
| --- | --- | --- |
| **Author** | **Service Domain & Technology Used** | **Outcomes & Limitations** |
| Kim et al. [1] | Smart transportation systems, route guidance | Enhances mobility via optimal route guidance, car/bike-sharing, and public transport efficiency |
| Wolniak & Grebski [8] | Smart transportation: MRT system, sustainable transport initiatives | Reduces traffic congestion and promotes sustainable transport |
| Kim et al. [1] | Smart community: ICT | Empowers individuals and regions through ICT |
| Hashim [9] | Smart community: Broadband infrastructure | Facilitates innovation in commerce, education, healthcare, and governance |
| Somayya & Rama [10] | Smart community: Collaborative ICT platforms (living and mobility) | Collaboration to solve urban issues in mobility and living |
| Kim et al. [1] | Smart living: Real-time information sharing | Helps citizens with daily challenges across smart domains |
| Vinod Kumar [12] | Smart living: Human development metrics | Smart people focus on HDI, learning, diversity, and adaptability |
| Shahzad Ashraf [13] | Smart living: Digital tools, online delivery systems | Smart education supports modern learning environments |
| Alam et al. [11] | Smart living: Home automation via smartphone/Bluetooth/Wi-Fi | Smart homes allow remote control of appliances like lights and security locks |
| Kim et al. [1] | Smart Environment: Real-time monitoring, autonomous systems | Enables efficiency in smart buildings, factories, energy systems |
| Vinod Kumar [12] | Smart Environment: Smart ecosystem platforms | Supports sustainability and community resilience during economic downturns |
| Ryalat et al. [5] | Smart Environment: Advanced manufacturing technologies | Smart factories drive manufacturing innovation |
| King & Perry [14] | Smart Environment: ICT in smart buildings | Optimizes building operations and energy usage |
| Dincer & Acar [15] | Smart Environment: Home Energy Management Systems (EMS) | Allows monitoring appliance usage; evaluates power and temperature data |

Port scanning is a reconnaissance technique used to identify vulnerabilities in systems by probing ports [19]. Although used by system administrators for diagnostics, it is also exploited by attackers to discover weaknesses. Port scans are categorized into vertical, horizontal, and block scans, depending on the scanning pattern and target type [19]. Brute-force attacks involve systematically guessing credentials until access is gained [20]. They are among the most prevalent cyberattack methods, especially against services like SSH, and often use precompiled dictionaries of username-password combinations [20]. These attacks are persistent and observed across various threat levels, often originating from the same IP addresses [20].

Table 2 presents a summary of common cyberattack methods observed in smart city environments.

## Honeypots in Cybersecurity

Honeypots are essential for cybersecurity operations due to their defensive ability to create simulated vulnerable systems to detect cyber attackers while collecting their attacking data and methods [6]. ”The honeypots have three main functionalities, namely Detection, Prevention, and Research. For the detection feature, the superior advantage of honeypots over other security tools in detecting cyber-attacks is their low rate of false detection. Regarding the prevention functionality, three aspects of the honeypots are considered: slowing down the adversary, creating a sense of danger for the adversary even if there are no security mechanisms deployed on the network, and wasting the adversary’s resources” [21].

**TABLE 2.** Summary of common attacks and insights

|  |  |  |  |
| --- | --- | --- | --- |
| **Author** | **Year** | **Common Attack** | **Insights** |
| Griffioen & Doerr [16] | 2020 | Mirai botnet | Mirai turns IoT devices into bots for DDoS attacks and notorious for the 2016 1.2 Tbps attack on major sites. |
| Hussain et al. [17], Gu & Liu [18] | 2020 | Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) | DoS is single source while DDoS has multiple agents and aims to disable systems/networks. |
| Lee et al. [19] | 2005 | Port scanning techniques | Used for identifying system vulnerabilities; patterns include vertical, horizontal, and block scans. |
| Sitawan et al. [20] | 2019 | Brute-force login methods | Systematically guesses credentials, often targets SSH, uses dictionaries of known combinations; persistent and recurring from same IPs. |

## Honeypot Deployment

A common method for deploying honeypots is to position them in strategic locations within a network. This approach aims to divert malicious activity away from critical systems while increasing the visibility of attacker be- havior. Research honeypots, for instance, have been deployed within university infrastructures to monitor and analyze attack patterns targeting educational networks. Similarly, a government agency utilized honeypots in a pilot project to study advanced persistent threats (APTs) directed at critical infrastructure [22]. In contrast, production honeypots are designed to seamlessly integrate with existing security systems, enhancing an organization’s ability to detect and respond to threats in real time [22]. By analyzing attacker behavior in these controlled environments, researchers have discovered new vulnerabilities and gathered valuable insights to improve security protocols [23].

## Types of Honeypot

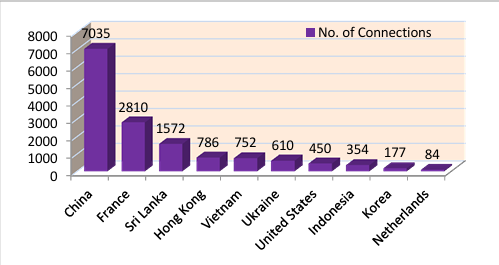
Honeypots are divided into three groups. They are high, low and medium interaction honeypots. “High-interaction honeypots emulate all parts of a system and all of its services. The advantage of high-interaction honeypots is that since there are many services for attack, it can be more convincing that the honeypot is a real system” [6]. Such honeypots become exploitable by attackers who subsequently utilize them to execute strong attacks on the network. The richness of the data collected makes these honeypots invaluable for threat intelligence, enabling a better understanding of the capabilities and intent of attackers by organizations [22]. “There are many honeypots which are high-interacted and one of them is SIPHON architecture, a Scalable High-Interaction Honeypot platform for IoT. SIPHON uses physical IoT devices connected via ‘wormholes’ distributed globally, allowing a few devices (less than 10) to appear as many across different IP addresses” [23].

Low-interaction honeypots emulate a specific part of an operating system and a certain number of services such as remote authentication services and file transfer services. These honeypots are systems that imitate particular TCP/IP model protocols. Their main advantage is that they consume relatively fewer resources than high-interaction honeypots and are easier to install [6]. Dionaea and Honeyd are examples of low-interaction honeypots that mimic a variety of services to draw in and examine malware; Dionaea is made to capture exploits that target services like SMB, HTTP, and FTP, while Honeyd can create virtual hosts on a network that mimic different operating systems and network configurations [24].

Between a low-interaction and high-interaction honeypot, a medium-interaction honeypot compromises some operating system validity to facilitate data analysis [24]. Organizations commonly utilize medium-interaction honeypots as a compromise since low-interaction honeypots have poor data quality and are unable to swiftly assess the wealth of information offered by high-interaction honeypots [24]. The complex nature of honeypots’ installation, configuration and maintenance makes them prone to a high level of security risks [24]. As an example of medium interaction honeypot, “Kippo imitates an SSH service in terms of being a deception trap. As the intruders access the SSH protocol and make attempts at logging into the emulated machine through brute-force attacks, the system collects all the login details and any other detailed logs into the database for analysis” [25].

## SSH(Secure Shell or Secure Socket Shell)

SSH ensures confidentiality, integrity, and authentication in remote access scenarios. It is commonly utilized alongside Secure Copy (SCP) for secure file transfers [25]. SSH servers operate on TCP port 22, where an initial connection between a client and server involves an exchange of SSH version information and encryption keys [25]. The authentication process determines whether the client is granted access or fails to authenticate, thereby reinforcing secure access control measures [25]. There have been a few research studies on using honeypot data to improve the security of SSH services using traditional security techniques and analytics methods, but most of the research in this field has only proposed honeypot models specifically for SSH-based attack detection. Figure 1 is the bar chart from a research paper [25] illustrating the number of SSH connection attempts recorded by the honeypot from various countries. This data suggests that China and France were the most significant sources of SSH-based interactions. Summary of smart city themes, features, and vulnerabilities is tabulated in Table 3.



**FIGURE 1.** Number of SSH connections in various countries

**TABLE 3.** Summary of smart city themes, features, and vulnerabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Author** | **Theme** | **Subtopic** | **Key Features** | **Vulnerabilities** |
| Akhtar & Thomas [2] | Smart Cities | IoT Infrastructure | Interconnected devices (sensors and actuators) for managing urban systems | Device heterogeneity, weak credentials, and protocol fragmentation |
| Kim et al. [1] | Smart Cities | Layered Architecture | Technology layer, communication layer, and service domains | Integration complexity and interoperability issues |
| Kim et al. [1]; Wolniak & Grebski [8] | Smart Transportation | Transport and Parking | Optimal routing, public transport enhancement | Data privacy and system security |
| Kim et al. [1]; Hashim [9] | Smart Community | Economy and Governance | ICT for innovation in commerce, education, governance | Needs strong infrastructure and collaboration |
| Kim et al. [1] | Smart Living | Healthcare, Homes, and Education | Real-time data sharing; smart homes with mobile control; e-learning | Data exposure and device vulnerabilities |
| Kim et al. [1]; Vinod Kumar [12] | Smart Environment | Buildings, Energy, and Factories | EMS, smart buildings, and factories to optimize energy and operations | Limited automation and data accuracy needed for EMS |
| Griffioen & Doerr [16] | Cyber Threats | Mirai Botnet | Large-scale IoT-based DDoS attack | Devastating service outages |
| Hussain et al. [17]; Gu & Liu [18] | Cyber Threats | DoS/DDoS Attacks | Single-source and multi-source attacks | Large-scale service disruption |
| Lee et al. [19] | Cyber Threats | Port Scanning | Reconnaissance via vertical, horizontal, and block scans | Used to identify vulnerabilities |
| Stiawan et al. [20] | Cyber Threats | Brute-force Attacks | Repeated login attempts using credential dictionaries | Highly persistent and targets SSH frequently |
| Moric et al. [6]; Javadpour et al. [21] | Honeypots & Cybersecurity | General Use | Simulate vulnerable systems to monitor and analyze attacker behavior | Low false detection rate and delays and deceives attackers |
| Dakic et al. [22]; Altunay [23] | Honeypots | Deployment Strategies | Strategically deployed to monitor and divert threats | Risk of misconfiguration, system exposure if isolated poorly, and added resource demands |
| Altunay [23] | Types of Honeypots | High-Interaction Honeypots | Full OS simulation like SIPHON with global wormholes | Resource-intensive and realistic for complex attack research |
| Moric et al. [6]; Z. Melese & Avadhani [25] | Types of Honeypots | Medium-Interaction Honeypots | Application-layer emulation only like Kippo simulates SSH | Captures detailed interactions without full system risk |
| Javadpour et al. [21] | Types of Honeypots | Low-Interaction Honeypots | Simulate basic services (TCP/UDP) like Honeyd | Ideal for large-scale deployment |
| Z. Melese & Avadhani [25] | SSH Protocol | Secure Remote Access | Confidentiality, integrity and authentication for remote login (TCP port 22) | Vulnerable to brute-force attacks if not well protected |
| Z. Melese & Avadhani [25] | Honeypot Research | Honeypot SSH Data | Studies show SSH honeypots log high traffic from countries like China and France | Indicates geographical attack trends and limited work on analytics use |

# CONCLUSION

This study reviewed the integration of IoT technologies within smart city infrastructures and the growing cyberse- curity risks associated with their deployment. The research study identified common cyberthreats like DDoS attacks, brute-force login attempts, and many more, and it highlighted important domains like smart environments, smart trans- portation, and smart living. Honeypots emerged as an effective tool for enhancing cyber defense, offering low false positive rates and valuable insights into attacker behavior [6]. The differentiation of honeypots into varieties with low, medium, and high interaction highlights their adaptability and significance in diverse deployment contexts [6]. The investigation of SSH-based threats further emphasized the utility of honeypots in monitoring real-world attack vectors, with empirical data pointing to consistent attack traffic from specific regions [25]. These results highlight the need for proactive, deception-based defenses in cybersecurity frameworks for smart cities. Future projects will in- clude the development and implementation of an SSH honeypot system made especially for smart city environments. By recording login attempts, attack patterns, and geographic origins, this honeypot will seek to identify and examine cyberthreats that target vital urban infrastructure. The information acquired will be useful in the creation of flexible security regulations and support larger initiatives to create safe, resilient smart cities.

# REFERENCES

1. K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, “Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey,” *Sensors* **23**(7), (2023).
2. S. Akhtar and J. Thomas, “Cyber forensics in the age of AI: Investigating cyber crimes with advanced multi-factor authentication and adaptive threat mitigation,” (2024).
3. A. Meijer and M. P. R. Bolívar, “Governing the smart city: A review of the literature on smart urban governance,” *International Review of Administrative Sciences* **82**(2), 392–408 (2016).
4. M. A. Alharbe, “Cyber security, forensics and its impact on future challenges in Saudi Arabia smart cities: Case study on modern urban planning and design,” *International Journal of Advanced Trends in Computer Science and Engineering* **9**(2), 2464–2470 (2020).
5. M. Ryalat, N. Almtireen, H. Elmoaqet, and M. Almohammedi, “The integration of two smarts in the era of industry 4.0: Smart factory and smart city,” in *2024 IEEE Smart Cities Futures Summit (SCFC 2024)*, 9–12 (2024).
6. Z. Moric, L. Mršić, Z. Kunic, and G. Šambic, “Honeypots in cybersecurity: Their analysis, evaluation and importance,” (2024).
7. B. S. Oliha and P. Obi, “Securing the smart city: A review of cybersecurity challenges and strategies,” *Engineering Science Technology Journal* **5**(2), 496–506 (2024).
8. R. Wolniak and W. Grebski, “Smart mobility in smart city – Singapore and Tokyo comparison,” *Scientific Papers of Silesian University of Technology Organization and Management Series* **176**, (2023).
9. H. Hashim, “E-government impact on developing smart cities initiative in Saudi Arabia: Opportunities and challenges,” *Alexandria Engineering Journal* **96**, 124–131 (2024).
10. M. Somayya and R. Ramaswamy, “Amsterdam smart city (ASC): Fishing village to sustainable city,” in *The Sustainable City XI* **1**, 831–842 (2016).
11. T. Alam, A. Salem, O. Alsharif, and A. Alhejaili, “Smart home automation towards the development of smart cities,” *Computer Science and Information Technologies* **1**(1), 17–25 (2020).
12. T. M. Vinod Kumar, “Smart environment for smart cities,” in *Advances in 21st Century Human Settlements*, 1–53 (Springer, 2020).
13. S. Ashraf, “A proactive role of IoT devices in building smart cities,” *Internet of Things and Cyber-Physical Systems* **1**, 8–13 (2021).
14. J. King and C. Perry, “Smart buildings: Using smart technology to save energy in existing buildings,” (2017).
15. I. Dincer and C. Acar, “Smart energy systems for a sustainable future,” *Applied Energy* **194**, 225–235 (2017).
16. H. Griffioen and C. Doerr, “Examining Mirai’s battle over the Internet of Things,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 743–755 (2020).
17. F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “IoT DoS and DDoS attack detection using ResNet,” (2020).
18. Q. Gu and P. Liu, “Denial of service attacks,” (2010).
19. C. B. Lee, C. Roedel, and E. Silenok, “Detection and characterization of port scan attacks,” (2005).
20. D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, “Investigating brute force attack patterns in IoT network,” *Journal of Electrical and Computer Engineering* **2019**, (2019).
21. A. Javadpour, F. Ja’fari, T. Taleb, M. Shojafar, and C. Benzaïd, “A comprehensive survey on cyber deception techniques to improve honeypot performance,” *Computers and Security* **140**, (2024).
22. Z. Moric, V. Dakic, and D. Regvart, “Advancing cybersecurity with honeypots and deception strategies,” *Informatics* **12**(1), (2025).
23. H. C. Altunay, “Analysis of cyber attacks using honeypot,” *Black Sea Journal of Engineering and Science* (2024).
24. S. T. Muntaha, F. Ashraf, I. Shahzad, and J. Iqbal, “Designing an adaptive honeypot for advanced cybersecurity threat detection,” *Spectrum of Engineering Sciences* **3**(5), 816–847 (2025).
25. S. Z. Melese and P. S. Avadhani, “Honeypot system for attacks on SSH protocol,” *International Journal of Computer Network and Information Security* **8**(9), 19–26 (2016).