Chapter 6
ACIDS: A Secure Smart City Framework and Threat Model

Soomaiya Hamid and Narmeen Zakaria Bawany

6.1 Introduction

More than 50% of today's world population dwells in urban areas to improve their quality of life, and this percentage is increasing with time [1]. The citizens' needs can be fulfilled efficiently if there is a well-established interconnected system to manage, maintain, and monitor the activities of the inhabitants [2]. Smart city is a human-friendly and efficient society that provides the core infrastructure for a quality life in almost all city-related facilities through smart city applications [3, 4]. These cities embrace information and communication technologies (ICT) to improve the quality and performance of civic services such as energy, municipal, health, transportation, safety, security, and utilities. Paroutis [5] affirmed that ICT involvement in urban services minimizes resource consumption, wastage, and overall cost. The smart city provisions an environment to connect all stakeholders and institutions by enabling intelligent and sustainable technologies and platforms like the Internet of Things (IoT) and cloud services. This promotes more efficient, convenient, and synchronized operations of urban infrastructure [6]. Therefore, smart cities have acquired more attention in the development and maintenance of a modern city [3].

Despite these benefits of interconnectivity and transparency, a smart city is prone to vulnerabilities and ultimately cybersecurity attacks. Smart city systems gather data from various sources, which include stakeholders and sensors, for the betterment of society. However, this sharing of data opens the opportunity for attackers to target a particular stakeholder or the entire system [7].

S. Hamid (✉) · N. Z. Bawany
Center for Computing Research, Department of Computer Science and Software Engineering, Jinnah University for Women, Karachi, Pakistan
e-mail: soomaiya.hamid@juw.edu.pk; narmeen.bawany@juw.edu.pk

I. Woungang, S. K. Dhurandher, *4th International Conference on Wireless, Intelligent and Distributed Environment for Communication*, Lecture Notes on Data Engineering and Communications Technologies 94, https://doi.org/10.1007/978-3-030-89776-5_6

Many cases have been reported in this regard as shown in Table 6.1. In early 2018, Atlanta was the victim of a virus named SamSam that severely affected their government agencies, hospitals, and big retailers. Colorado Department of Transportation of Atlanta (CODT) reported that SamSam shutdown more than 20,000 computers and pushed them into the dark ages where people had pen and paper to do their daily business [8]. Victims were then asked for bitcoins to get their files back. The SamSam was also used to attack Indiana [9] which disrupted the US hospital management system by encrypting the files and renamed them with the phrase "I'm sorry." The hospital management operations were halted for 2 days. This system was restored after paying 4 bitcoins worth $55,000 but took many days to smooth the hospital management operations.

In Czech Republic,[1] a cyberattack was triggered during the COVID-19 pandemic. Brno University Hospital's smart system was hacked which was one of the largest coronavirus centers in the Czech Republic. The attack paralyzed the whole IT system of the hospital. Attackers announced publicly that all surgeries are canceled. Hospital management failed to operate the COVID-19 testing system, and patients were shifted to other hospitals.

In 2018, Marriott[2] reported that data of 383 million travelers have been compromised in "a breach of Marriott's Starwood Preferred Guest (SPG) database." The investigation reveals that this data breach happened because of a few unencrypted passport numbers. Moreover, the report said that the attacker had unauthorized access since 2014. This attack not only revealed the payment details but revealed personal sensitive information. In 2015, Fiat Chrysler Automobiles declared that their Jeep Cherokee has been hacked by cybercriminals [10]. Therefore, the company had to recall 1.4 million cars. Afterward, the company had to install a security patch in every vehicle physically to secure the system.

In South Carolina [10], a mother noticed that the baby video monitor is moving around the room instead of focusing on the baby bassinet. First, she thought that some family member was controlling it with a smartphone app, but later she realized that it is being hacked and someone is collecting images of the personal activities.

The literature encompasses many smart city frameworks [11, 12], but most of the work is limited to an efficient interconnected architecture leaving behind its security aspect. However, there are specific smart city architectures that include security for a particular application only [13–15].

The rising number of attacks, along with the diversity in their types, clearly shows that we need new approaches and frameworks which prioritize the security aspect. Therefore, we proposed a layered smart city framework—ACIDS (Application, Communication, Infrastructure, Data, and Stakeholders)—that embeds security in

[1] https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

[2] https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (accessed 10.14.2020).

Table 6.1 Popular attacks on smart city

Year	Target/victim	Affected ACIDS layer	Type of attack	Effect of attack
2020	Brno University Hospital management system, Czech Republic (https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/)	Communication layer	Ransomware attack	Hospital management failed to operate the COVID-19 testing system and patients' surgeries
2020	Worldwide Personal Privacy (https://www.who.int/about/communications/cyber-security)	Stakeholder layer	Phishing attack	The attacker sent fake invoices for requesting funds for COVID-19 victims, asked for personal information, posing himself as WHO (World Health Organization)
2019	New Orleans (https://www.pymnts.com/innovation/2020/secure-smart-cities-cybercriminals/)	Communication layer	Ransomware attack	Attack forced to the shutdown of thousands of systems of the city
2019	US hospital management system, Indiana (https://www.trendmicro.com/vinfo/tr/security/news/cyber-attacks/samsam-ransomware-hits-us-hospital-management-pays-55k-ransom)	Data layer	Ransomware attack	Attackers encrypted and renamed the files. The hospital management operations were halted for 2 days
2018	Government agencies, hospitals, and big retailers, Atlanta (https://www.iotworldtoday.com/2018/04/05/smart-city-security-atlanta-cyberattack-cripples-city/)	Infrastructure layer	Ransomware attack	Shutdown more than 20,000 computers
2018	Marriot Hotel, Maryland, USA (https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/)	Data layer	Ransomware attack	Attack revealed the 383 million travelers' payment details and sensitive information

(continued)

Table 6.1 (continued)

Year	Target/victim	Affected ACIDS layer	Type of attack	Effect of attack
2016	USA (https://news.softpedia.com/news/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks-505722.shtml#ixzz4CsbxFc4A)	Application layer	DDoS attack	Attackers strive through CCTV-based botnet and occupied the server availability through illegitimate traffic by generating about 50,000 HTTP requests per second
2015	Fiat Chrysler Automobiles, North America (https://www.bbc.com/news/technology-33650491)	Communication layer	Remote hacking attack	A smart "Jeep Cherokee" has been hacked by cybercriminals
2015	Personal Security, South Carolina (https://www.npr.org/sections/thetwo-way/2018/06/05/617196788/s-c-mom-says-baby-monitor-was-hacked-experts-say-many-devices-are-vulnerable)	Infrastructure layer	Device hijacking	The baby video monitor was hacked, and the attacker was collecting images of the personal activities by moving the camera around the entire room instead of focusing on the baby bassinet
2015	Electric Power Grid, Ukraine (https://www.eenews.net/stories/1060040399/)	Infrastructure layer	Trojan horse	Attackers successfully hacked the power grid

each of its layers. Moreover, various threats respective to each layer and their consequences are presented in detail.

The major contributions of this chapter are as follows:

- We present a detailed comparison of existing smart city security frameworks.
- We propose a secure layered framework ACIDS for smart city.
- We present a threat model for a smart city that identifies major threats in each layer.

The rest of the chapter is organized as follows. Section 6.2 discusses the taxonomy of previous research work in this domain. ACIDS framework and its threat model are described in Sect. 6.3. Section 6.4 concludes the chapter and outlines future directions.

6.2 Related Literature

To address the cybersecurity threats in a smart city, an Anomaly Detection loT (AD-IoT) [16] system was proposed. AD-IoT intelligently detected anomalies by the Random Forest machine learning algorithm. This system also detected anomalies over compromised loT devices at distributed fog nodes. Researchers [17] have provided analysis and taxonomy of security and privacy challenges in the IoT layer only. Makhdoom et al. [18] present a blockchain-based framework "PrivySharing," which provides privacy and security of data sharing over a smart city network. Dong et al. [14] presented cyber issues in smart energy applications. Cyber-security challenges through a vulnerability assessment for the deployment of smart streetlight systems are presented. Brown and Seuwou [19, 20] presented smart city security and privacy challenges regarding mobility and transportation systems. Privacy and security challenges in smart healthcare are also discussed in various research [21–23]. Vitunskaite et al. [24] presented the role of IEEE standards and regulatory framework for cybersecurity with a comparative case study of three different countries. Many researchers [1, 25] presented various cybersecurity threats to smart city applications. To provide a secure platform for IoT devices, Chakrabarty and Engels [26] introduced four-block architecture.

Braun and Habibzadeh [21, 27] highlighted data privacy issues of a smart city and discussed the critical issues of cloud sharing platforms in a smart city. Furthermore, AlDairi and Tawalbeh [28] presented data privacy issues and smart city infrastructure challenges.

Cybersecurity challenges have been studied extensively in the smart city context [29]. We have examined more than 10 research papers in detail, and their findings are summarized in Table 6.2. Typically, previous studies are limited to a particular domain within a smart city, such as smart grid, smart traffic control system, VANETs, etc.

Table 6.2 A taxonomy of the research papers in security of smart city

Research paper	Smart city framework	Smart city framework with cybersecurity	Infrastructure layer security	Communication layer security	Data layer security challenges	Application layer security	Stakeholder layer security
[18]	✗	✗	✓	✗	✓	✗	✓
[19]	✗	✗	✗	✗	✗	✓	✗
[20]	✗	✗	✗	✗	✗	✓	✗
[16]	✗	✗	✓	✗	✗	✗	✗
[21]	✗	✗	✗	✗	✗	✓	✗
[25]	✗	✗	✓	✗	✗	✗	✗
[30]	✓	✗	✗	✗	✗	✗	✗
[27]	✗	✗	✗	✗	✓	✗	✗
[28]	✗	✗	✓	✗	✓	✗	✗
[31]	✗	✗	✗	✗	✗	✓	✗
[14]	✗	✗	✗	✓	✗	✓	✗
[26]	✗	✗	✗	✓	✓	✗	✗
[17]	✗	✗	✓	✓	✗	✗	✗
ACIDS	✓	✓	✓	✓	✓	✓	✓

In this study, we propose a layered model to cover all the domains of a smart city. Vulnerabilities corresponding to each layer are identified, and the threat model is also presented.

6.3 ACIDS: The Proposed Framework

Smart city applications are developed to improve the management of urban areas. A huge and complex network exists to control, maintain, and provide services in a smart environment. Thousands of sensors and IoT devices are deployed that generate a huge amount of data. The data is collected, processed, and analyzed by applications to provide various services to citizens. This creates a highly complex and tightly knitted architecture. To classify the relation among these attributes, this chapter introduced a layered framework for smart cities, titled ACIDS (Application, Communication, Infrastructure, Data, and Stakeholders) as shown in Fig. 6.1. The framework has five layers that represent the overall architecture of the smart city.

6.3.1 *Infrastructure Layer*

The infrastructure layer serves as a primary layer that constructs an entire framework to provide smart services to the citizens. This layer typically exists as a physical

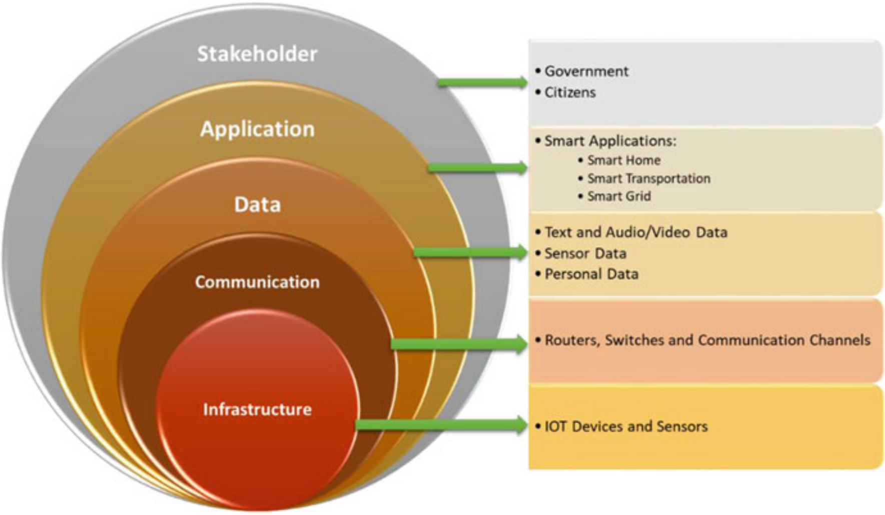

Fig. 6.1 Smart city layered model

platform that involves hardware such as actuators, IoT sensors, and other devices. This layer has a risk of physical damage or hijacking of the devices' control.

6.3.2 Communication Layer

This layer encompasses all the communication channels that can be used within a smart city. These communication channels include Wi-Fi, Ethernet, optical fiber, and broadband communications that are deployed across the smart city. Every device that is connected in smart city architecture needs strong communication to cover a wide geographical area. This huge and variable amount of data cannot communicate over a single communication technology. Therefore, multiple communication channels are used.

6.3.3 Data Layer

The IoT devices from the infrastructure layer generate a huge amount of data which includes structured and unstructured text, images, videos, and audios [32]. The data is generated from different smart city applications, such as transportation, utilities, health, business, energy, and waste management systems. Data layer carries big data platforms, to store, analyze, and process the data to provide ease to ICT projects of smart city. More data needs more computation power [33]. However, this data analysis plays an important role to build a city, smart. All applications of the smart city share data among them to provide better solutions to improve citizen's lives.

6.3.4 Application Layer

The application layer provides interaction between users and applications. Smart city applications facilitate users by providing ease and services to help them in performing daily life activities. This layer is responsible for collecting real-time responses of users to process further. These applications are developed for a vast variety of operations to solve city-related problems and help to make the city developed and safer.

6.3.5 Stakeholders

A stakeholder is a person or a group of persons that have a common interest in a system. They can either affect or be affected by the system. Smart cities help the government to provide a quality life to its citizens. Therefore, the two major categories of stakeholders that exist in a smart city are government and citizens. However, this part is least considered by the researchers of smart cities in their studies. It is important to emphasize that stakeholder roles must be established before developing any smart city plan because these players have the most influence on city initiatives and operations.

6.4 ACIDS Threat Model

A smart city provides complete connectivity among different sectors of modern society. Therefore, the data, services, and applications are integrated to build a strong smart city. This integrated nature of a smart city may attract many attackers to hack or disrupt the functions of a smart city, but due to its complex network, this becomes too difficult to identify which area of the network is vulnerable and prone to attacks. To overcome this difficulty, this research paper proposed an ACIDS threat model, which defines particular threats over each layer of ACIDS as shown in Fig. 6.2.

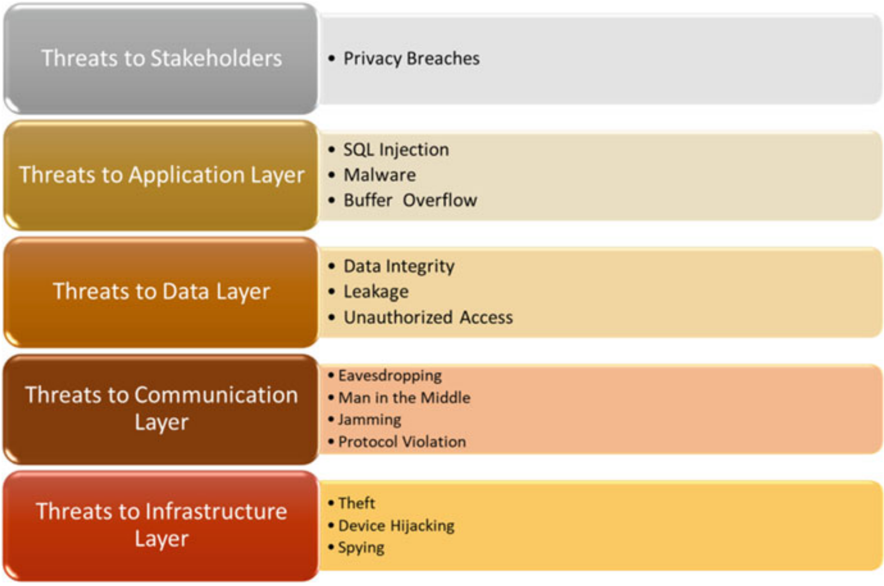

Fig. 6.2 ACIDS threat model

6.4.1 Threats to Infrastructure Layer

The infrastructure layer is a physical layer of smart city architecture. The layer can not only be compromised remotely but is also vulnerable to physical attacks. Therefore, the infrastructure layer has to be protected from both physical attacks and cyber-attacks. The following section discusses major attacks on the infrastructure layer, which defines how this layer can be targeted by attackers.

6.4.1.1 Theft

Theft is a very common attack that is performed by stealing tangible technological equipment. It affects the systems' availability and confidentiality. This kind of attack not only originates financial and reputational losses but also creates loopholes for attacks like impersonation and identity theft. In June 2019, [34] 20 laptops from the administration building of The University of Western Australia (UWA) were stolen. UWA reported that around 100,000 students, who have applied to study in the university from 1988 to 2018, are at risk due to this data breach.

6.4.1.2 Device Hijacking

Device hijacking is an attack in which an attacker gets control of the device. In a smart city, sensors and smart devices are the main assets for smart operation. If an attacker gets effective control of these devices, it can create havoc in the system. The identification of these attacks is difficult because of the attacker's movements [25]. If an attacker is generating a passive attack by only observing data and does not respond or alter basic functionality, the system administrator will not be able to detect the attacker's activities. This would be destructive for any smart city operation. The complete breakdown of smart city operations such as energy, municipality, water supply, or electrical power failure can be caused by device hijacking [35]. In December 2015, Ukraine faced a complete blackout due to the attack on the smart electricity system. In this attack, attackers have successfully hacked the power grid and left the three big energy distribution companies helpless to sustain their positions [36].

6.4.1.3 Spying

Security cameras are typically used in smart city applications for surveillance. A camera which is installed for security purposes becomes vulnerable when it is hacked and controlled by malicious users [37]. Attackers can get access to personal data and images or they can spy on people. If a camera is installed to cover the cashier's desk or at the banks where people use their cash and PINs fearlessly, a hacker could spy on people and plan a robbery [28]. Hackers can also replace the real-time streaming of a compromised camera with a tempered video or can completely block the video [38, 39].

6.4.2 Threats to Communication Layer

Communication layer keeps the smart city components interactive, by which devices and applications can communicate with each other. This layer is highly prone to attacks because it is exposed to all the layers of ACIDS. This layer is vulnerable to network traffic interception. These attacks may modify the communication to impersonate the user or service, or simply capture the communication channel so that they can perform malfunctions later with this information. Communication layer attackers also manipulate protocols to violate their rules and policies and create a way toward unauthorized access. A few of the communication layer attacks are described below:

6.4.2.1 Eavesdropping

Eavesdropping is an attack in which an attacker listens to all kinds of communication between users, applications, and communication channels. This unauthorized reader only reads the data without any interruption or tempering [40]. By eavesdropping, an attacker can perform a traffic analysis of confidential information about participants, pinpoint their location, or record their private conversations [41]. These kinds of attacks are not only threatening for smart applications but can also affect the privacy and security of all stakeholders.

6.4.2.2 Man in the Middle Attack

In cybersecurity Man-In-The-Middle (MITM) is a very common attack that takes an attacker one step forward from eavesdropping. Attack intercept communication among users and temper data during transmission. This may falsify the operators' actions and interrupt or spoof communication between two systems [42]. There are two phases to make the MITM attack successful; interception, and decryption.

Interception—in the first step, legitimate traffic is diverted to the attacker's network before reaching the destination. These attacks can be executed by creating free malicious Wi-Fi for the public. Once a victim connects with this unprotected network, the attacker gains full visibility of any online data exchange. Following are the few active approaches to intercept communication between two different nodes [43]. (a) IP Spoofing—is a technique in which an attacker alters the packet header to disguise himself as a legitimate application. As a result, when a user attempts to access that particular application, the attacker's website gets connected.

So that all the user's activities are shared with the attacker without consent. (b) ARP Spoofing—is an activity in which attackers disguise their own MAC address as a legitimate user's MAC address. The attacker generates a fake ARP message to inform the network that this MAC address is not linked with the user's IP address on a local area network. As a result, all data sent to that particular IP address is transmitted to the attacker's site. (c) DNS Spoofing—is a process of DNS cache poisoning, in which an attacker infiltrates a DNS server, redirecting the particular website address to its IP address. As a result, all users are directed to the fake site.

Decryption—once an attacker gets access to the user's communication data by interception, a two-way SSL communication traffic requires a process of decryption. Many methods exist for this purpose; few of them are discussed here. (a) HTTPS spoofing—is a technique in which a victim's browser receives a fake certificate after the interception phase. This certificate contains digital signatures associated with the compromised application. Therefore, the browser verifies the signatures from the existing list of trusted sites. As a result, the data is sent to the attacker's address from the victim's system. (b) SSL hijacking—is an activity that is performed during TCP handshake. The attacker shares forged authentication keys with the user and application both. This disguises a secure connection while the entire connection is under the control of the attacker. (c) SSL stripping—downgrades an HTTPS connection to HTTP by intercepting the TLS authentication sent from the application to the user. The attacker sends an unencrypted version of the application's site to the user while maintaining the secured session with the application. Meanwhile, the user's entire session is visible to the attacker.

6.4.2.3 Jamming

Jamming is one of the simplest attacks, which makes the communication channel occupied via malicious activities such that the legitimate nodes are unable to connect. The attacker generates interference signals to block communication channels and disrupt normal operations, due to which not only is performance degraded, but it also damages the control system. This attack mostly works effectively with wireless channels [44].

There are two categories of jamming attacks: active and reactive. Active Jammer's goal is to keep the channel busy regardless of whether the channel is being used or not. They continuously send strong radio signals which increase the noise interference at the receiver's side. Reactive Jammers notice the activity over the communication channel and send signals only when the channel is being used by legitimate users [45].

6.4.2.4 Protocol Violation

Ping of death attack—allows attacker attempts to crash, destabilize, or freeze the targeted smart system or service by sending malformed or oversized packets using a simple ping command. The Internet Protocol (IP) defines a maximum packet length of 65,536 bytes. Usually, networks do not support packets of that length. However, sending a ping packet larger than 65,535 bytes violates the Internet Protocol. Fragmentation occurs on larger packet sizes by splitting the packet into smaller chunks. When the target system attempts to reassemble the fragments and ends up with an oversized packet, a memory overflow could occur and lead to various system problems including the crash [46]. Ping of death attacks was particularly effective because the victim's identity could be easily spoofed. Also, an attacker would need no detailed knowledge of the machine he/she was attacking, except for its IP address.

Smurf Attack—is a type of Distributed Denial of Service attack (DDoS) in which a large number of Internet Control Message Protocol (ICMP) packets are broadcasted to the computer network. This malware generates a fake echo request containing a spoofed source IP, which is the target server IP address. As the request is broadcasted so every host connected to that network will respond with an echo ICMP packet to the spoofed server IP address. This amplifies the effect of the Smurf attack and makes the targeted server bring down. Due to this, network performance is degraded and servers become unavailable for legitimate traffic [29].

TCP SYN Flood Attack—exploits TCP three-way handshake to consume targeted server resources and render it unavailable for the entire network. TCP SYN attack behaves like a DDoS attack by sending TCP connection requests faster than the targeted machine can process [47].

6.4.3 Threats to Data Layer

A strong data sharing and dependency among smart city applications leads to issues of data security and privacy over smart cities. Attackers try to expose, destroy, alter, or steal data to generate further attacks. From unauthorized access, attackers target to disrupt the smart city operations.

6.4.3.1 Data and Identity Theft

Data is an important part of every ICT project or system, and the way it is stored and shared shows the security concerns of the administration. By default smart gadgets and devices generate unprotected data such as simple surveillance cameras, parking garages sensors, smart traffic controls, personal fitness gadgets, and so on. Due to the inheritance property of interconnectivity among smart city applications, an ample amount of data is shared by different applications [48]. This allows data to be used by other smart city applications, and attackers take advantage by making fraudulent transactions. Moreover, the attacker also learns from the previously shared data by the victim and uses it for impersonation [49].

6.4.3.2 Unauthorized Access Control

Most of the systems are initiated by capturing users' credentials. It gives the impression that this system is secure and no one can access it, except authorized users [50]. But unfortunately, this so-called secure system becomes vulnerable, when security protocols are not fully implemented leading to attacks such as weak authentication schema and tampering with authentication tokens.

6.4.3.3 Default or Test Accounts

Default accounts are often used to initiate a system for the first configuration. System administrators leave that account as it is and create more accounts to use the system. When an attacker discovers the installed software at the victim's side, it is quite easy to find out the default accounts of a standard system to login. If the system administrator did not remove the default account, the attacker gets access from this loophole [51]. Moreover, test accounts are created by developers during the development to test the system. Test accounts, if not deleted or disabled after deployment, create a backdoor for attackers [52].

6.4.4 Threats to Application Layer

The Application Layer of ACIDS plays an important role to build a bridge between users and computers. This is the first layer that can be affected by malware. Cybercriminals are constantly enhancing their abilities to approach new application layer threats. This layer includes an attack on applications and services smart services unavailable to legitimate users. Some common attacks are discussed below:

6.4.4.1 DoS and DDoS Attack

DoS attack is defined as a Denial of Service attack in which a server is flooded by illegitimate requests from a robotic client with TCP and UDP packets. Whereas a DDoS attack is a Distributed Denial of Service attack in which a server is targeted by multiple illegitimate clients from different regions. DDoS is more dangerous than DoS because of its distributed nature [53].

These multi-vector attacks boost the application layer to high risk by modifying their payload patterns continuously due to which the attack becomes more complex and undetectable. Application Flooding and Web server maximum threads are also types of Denial of Service attacks [54].

6.4.4.2 SQL Injection

SQL Injection (SQLi) is an attack that injects malicious SQL queries and executes them. SQL server controls the web application from the backend and does not want interference from outside the web application. To make sure of the security of the SQL server, developers apply security measures. But unfortunately, attackers bypass these security measures because of the vulnerabilities of the system [55]. The attacker injects SQL queries to show, add, modify, and delete records in the database.

After attacking the system by SQL injection, attackers can transfer data between application and database [56]. Due to this, the attacker pushes the device to compromise the security of the smart city by performing false operations [57].

6.4.4.3 Application Workflow

Many application developers have an assumption that the user will follow the application flow as designed. But attackers have a very different mindset to bypass these legal and smooth flow of an application. Many applications of smart cities are interconnected and transfer data to each other. Therefore, if an insecure application is fetching data from a secure one with a legal flow, a loophole is created through which an attacker can penetrate that secure application [58].

6.4.5 Threats to Stakeholders (TS)

The roles and responsibilities of stakeholders vary with their category, that is, government and citizens. Government plays an essential and critical role in a smart city to control and manage the city infrastructure and provide services to its citizens. Citizens' roles include all users of the smart city system.

Both citizens and government administrators are affected by any security breach or attack. The extent of damage/loss is dependent on the activity of an attacker, infected application, and the role of the stakeholder. If a smart home application is compromised, citizens will suffer more than the government. In contrast, if a smart taxation system is compromised and a hacker makes false entries, the government's revenue sheets are compromised.

Smart city services must incorporate cybersecurity solutions to identify and mitigate threats. This works best when cybersecurity becomes a part of the legal city plans. Singapore passed a bill to ensure that proactive steps must be followed by the operators to secure data and the infrastructure of a smart city [59]. The government of Singapore also initiated cybersecurity awareness programs in universities, government, and private sector institutions. Therefore, they are becoming a Smart Nation by developing a security mindset. Organizations in Singapore have to implement a cybersecurity regulatory framework that consists of policies and procedures to identify cybersecurity threats, and in case of any incident, they can report under law sections.

London's mayor has launched a "London City Challenge" to make London the world's best and unique smart city to live in [60]. With all other activities, he also invested in London Digital Security Centre [61]. This is a joint venture between the Mayor of London, the Metropolitan Police Service, and the City of London Police. By this effort, London protects its citizens and business from cyber-crimes on an enterprise level. They also created an Information Security cell to support their public bodies from credential thefts. Moreover, Hague Security Delta [62] is also serving more than 200 organizations in Europe by working together to establish a secure environment.

The involvement of all stakeholders either citizens or government is necessary to create a culture of cybersecurity across the smart city. The establishment of a crime-free ecosystem for a smart city can only be achieved by implementing security policies in the public and private sector organizations.

With all the possible anti-malware activities, sometimes only users become a backdoor for attracting attackers. Users can be tricked by attackers, by tempting them to click on malware to install via advertisements or popups. Novice users are more often trapped in fake and phishing certificate sites leading to security breaches and data leaks. Weak passwords are also one of the major sources to invite attackers. Typically, users set weak passwords as they are easy to recall, but dictionary and brute-force attacks can break them easily.

6.5 Conclusion

A smart city tends to improve the quality of life of its citizens by connecting all stakeholders, that is, government, community, and citizens. Although this connectivity is beneficial in various ways, it brings about many security challenges as it enhances the threat landscape. The strongly knitted smart city systems are more vulnerable to attacks. This research presents a layered framework for smart city security—ACIDS.

ACIDS is a layered architecture that segregates smart cities into five layers, that is, Infrastructure, Communication, Data, Application, and Stakeholders. This chapter also proposed an ACIDS threat model that identifies various threats and each layer, such that developers can incorporate an exclusive/specific security mechanism for each layer. The layered architecture proposed in this chapter is highly beneficial for developing secure smart city systems. The threat model presented in this chapter can help in reducing the vulnerabilities significantly.

This framework can be applied to various use cases of smart cities such as Smart Grid, Smart Water and Waste Management, Smart Transportation, etc. In the future, we would like to implement these systems using the proposed ACIDS framework along with the security mechanisms that protect from the threats at each layer.

References

1. Khatoun, R., & Zeadally, S. (2016). Smart cities: Concepts, architectures, research opportunities. *Communications of the ACM, 59*, 46–57. https://doi.org/10.1145/2858789
2. Hollands, R. G. (2008). Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City, 12*, 303–320. https://doi.org/10.1080/13604810802479126
3. Su, K., Li, J., & Fu, H. (2011). Smart city and the applications. In *International conference on electronics, communications and control* (pp. 1028–1031).
4. Lazaroiu, G. C., & Roscia, M. (2012). Definition methodology for the smart cities model. *Energy, 47*, 326–332. https://doi.org/10.1016/j.energy.2012.09.028
5. Paroutis, S., Bennett, M., & Heracleous, L. (2014). A strategic view on smart city technology: The case of IBM smarter cities during a recession. *Technological Forecasting and Social Change, 89*, 262–272. https://doi.org/10.1016/j.techfore.2013.08.041
6. Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. In *ACM international conference proceeding series* (pp. 282–291). ACM Press.
7. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*, 491–497. https://doi.org/10.1016/j.jare.2014.02.006
8. Kraszewski, K. (2019). SamSam and the silent battle of Atlanta. In *International conference on cyber conflict, CYCON*. NATO CCD COE Publications.
9. Zimba, A., & Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research, 4*, 3–31. https://doi.org/10.1007/s41125-019-00039-8
10. Williams, M. (2015). 1.4 million cars that could be hacked are recalled by Fiat Chrysler In *PCWorld from IDG*. https://www.pcworld.com/article/2952592/chrysler-recalls-14m-cars-that-were-vulnerable-to-remote-hacking.html
11. Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An information framework for creating a smart city through internet of things. *IEEE Internet of Things Journal, 1*, 112–121. https://doi.org/10.1109/JIOT.2013.2296516
12. Bawany, N., & Shamsi, J. (2015). Smart city architecture: Vision and challenges. *International Journal of Advanced Computer Science and Applications, 6*(11), 246–255. https://doi.org/10.14569/ijacsa.2015.061132
13. Ding, D., Conti, M., & Solanas, A. (2016). A smart health application and its related privacy issues. In *Smart city security and privacy workshop* (pp. 11–15). IEEE.
14. Jin, D., Hannon, C., Li, Z., et al. (2016). Smart street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security. *The Electricity Journal, 29*, 28–35. https://doi.org/10.1016/j.tej.2016.11.011
15. Khurana, H., Hadley, M., Lu, N., & Fryncke, D. A. (2010). Smart-grid security issues. *IEEE Security and Privacy, 8*, 81–85. https://doi.org/10.1109/MSP.2010.49
16. Alrashdi, I., Alqazzaz, A., Aloufi, E., et al. (2019). AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In *9th annual computing and communication workshop and conference* (pp. 305–310). IEEE.
17. Babar, S., Mahalle, P., Stango, A., et al. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). In *Communications in computer and information science* (pp. 420–429). Springer.
18. Makhdoom, I., Zhou, I., Abolhasan, M., et al. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security, 88*, 101653. https://doi.org/10.1016/j.cose.2019.101653
19. Brown, M. (2020). Smart transport. In *Smart cities in application* (pp. 802–813). Springer.
20. Seuwou, P., Banissi, E., & Ubakanma, G. (2020). *The future of mobility with connected and autonomous vehicles in smart cities* (pp. 37–52). Springer.

21. Habibzadeh, H., & Soyata, T. (2019). Toward uniform smart healthcare ecosystems: A survey on prospects, security, and privacy considerations. In *Connected health in smart cities* (pp. 75–112). Springer.
22. Ranjith, J., & Mahantesh, K. (2019). Privacy and security issues in smart health care. In *4th international conference on electrical, electronics, communication, computer technologies and optimization techniques, ICEECCOT 2019* (pp. 378–383). Institute of Electrical and Electronics Engineers Inc.
23. Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019). Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Research Review, 4*, 149–168. https://doi.org/10.1108/prr-08-2019-0027
24. Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security, 83*, 313–331. https://doi.org/10.1016/j.cose.2019.02.009
25. Chen, J., Zuo, C., Diao, W., et al. (2019). Your IoTs are (not) mine: On the remote binding between IoT devices and users. In *IEEE/IFIP international conference on dependable systems and networks* (pp. 222–233). IEEE.
26. Chakrabarty, S., & Engels, D. W. (2016). A secure IoT architecture for Smart Cities. In *Annual consumer communications and networking conference* (pp. 812–813). IEEE.
27. Qamar, T., Bawany, N. Z., Javed, S., & Amber, S. (2019). Smart city services ontology (SCSO): Semantic modeling of smart city applications. In *Proceedings - 2019 7th international conference on digital information processing and communications, ICDIPC 2019* (pp. 52–56). Institute of Electrical and Electronics Engineers Inc.
28. Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society, 39*, 499–507. https://doi.org/10.1016/j.scs.2018.02.039
29. Aldairi, A., & Tawalbeh, L. (2017). Cyber security attacks on smart cities and associated mobile technologies. *Procedia Computer Science, 109*, 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391
30. Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine, 55*, 51–59.
31. Bawany, N., & Shamsi, J. (2019). SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. *Journal of Network and Computer Applications, 145*, 102381. https://doi.org/10.1016/J.JNCA.2019.06.001
32. Chiesa, G. (2020). *Data, properties, smart city* (pp. 169–190). Springer.
33. Chamoso, P., González-Briones, A., De La Prieta, F., et al. (2020). Smart city as a distributed platform: Toward a system for citizen-oriented management. *Computer Communications, 152*, 323–332. https://doi.org/10.1016/j.comcom.2020.01.059
34. Hiatt, B. (2019). UWA student data may be compromised after laptop theft—The West Australian. In *WA News*—Educ. https://thewest.com.au/news/wa/uwa-student-data-may-be-compromised-after-laptop-theft-ng-b881272938z
35. Al-Taleb, N., Saqib, N. A., Atta-ur-Rahman, & Dash, S. (2020). Cyber threat intelligence for secure smart city. arXiv.
36. Adepu, S., Kandasamy, N. K., Zhou, J., & Mathur, A. (2020). Attacks on smart grid: Power supply interruption and malicious power generation. *International Journal of Information Security, 19*, 189–211. https://doi.org/10.1007/s10207-019-00452-z
37. Mohammed, F., Idries, A., Mohamed, N., et al. (2014). UAVs for smart cities: Opportunities and challenges. In *International conference on unmanned aircraft systems, ICUAS* (pp. 267–273). IEEE Computer Society.
38. Valente, J., & Cárdenas, A. A. (2015). Using visual challenges to verify the integrity of security cameras. In *ACM international conference proceeding series* (pp. 141–150). Association for Computing Machinery.
39. Takefuji, Y. (2018). Connected vehicle security vulnerabilities [commentary]. *IEEE Technology and Society Magazine, 37*, 15–18.

40. Baig, Z. A., Szewczyk, P., Valli, C., et al. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*, 3–13. https://doi.org/10.1016/j.diin.2017.06.015
41. Qu, Y., Nosouhi, M. R., Cui, L., & Yu, S. (2018). Privacy preservation in smart cities. In *Smart cities cybersecurity and privacy* (pp. 75–88). Elsevier.
42. Dua, A., Kumar, N., Das, A. K., & Susilo, W. (2018). Secure message communication protocol among vehicles in smart city. *IEEE Transactions on Vehicular Technology, 67*, 4359–4373.
43. Maruˇ, M. (2016). Automatization of MitM attack for SSL/TLS decryption original connection. In *Excel@FIT 2016, student conference of innovation, technology and science in it* (pp. 2–8).
44. Niu, J., Ming, Z., Qiu, M., et al. (2015). Defending jamming attack in wide-area monitoring system for smart grid. *Telecommunication Systems, 60*, 159–167. https://doi.org/10.1007/s11235-014-9930-3
45. Garcia-Font, V., Garrigues, C., & Rifà-Pous, H. (2016). A comparative study of anomaly detection techniques for smart city wireless sensor networks. *Sensors, 16*, 868. https://doi.org/10.3390/s16060868
46. Abdollahi, A., & Fathi, M. (2020). An intrusion detection system on ping of death attacks in IoT networks. *Wireless Personal Communications*, 1–14. https://doi.org/10.1007/S11277-020-07139-Y
47. Kepceoglu, B., Murzaeva, A., & Demirci, S. (2019). Performing energy consuming attacks on IoT devices. In *27th telecommunications forum, TELFOR 2019*. Institute of Electrical and Electronics Engineers Inc.
48. Choenni, S., Bargh, M. S., Roepan, C., & Meijer, R. F. (2016). Privacy and security in smart data collection by citizens. In *Public administration and information technology* (pp. 349–366). Springer.
49. Ghosh, D., Ae Chun, S., Adam, N. R., & Shafiq, B. (2016). Big data-based smart city platform: Real-Time crime analysis. In *ACM international conference proceeding series* (pp. 58–66). ACM.
50. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297. https://doi.org/10.1016/j.scs.2018.02.014
51. Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional, 14*, 28–33. https://doi.org/10.1109/MITP.2012.72
52. Yu, W. D., Supthaweesuk, P., & Aravind, D. (2005). Trustworthy Web Services based on testing. In *Proceedings - SOSE 2005: IEEE international workshop on service-oriented system engineering* (pp. 167–177).
53. Bawany, N., & Shamsi, J. (2016). Application layer DDoS attack defense framework for smart city using SDN. In *Proceedings of the third international conference on computer science, computer engineering, and social media* (pp. 1–9). IEEE.
54. Sonar, K., & Upadhyay, H. (2016). An approach to secure Internet of Things against DDoS. In *Proceedings of international conference on ICT for sustainable development* (pp. 367–376). Springer.
55. Kim, J. M., Jeong, H. Y., Cho, I., et al. (2014). A secure smart-work service model based OpenStack for cloud computing. *Cluster Computing, 17*, 691–702. https://doi.org/10.1007/s10586-013-0251-1
56. Ahamed, J., & Rajan, A. V. (2017). Internet of Things (IoT): Application systems and security vulnerabilities. In *International conference on electronic devices, systems, and applications*. IEEE Computer Society.
57. Choi, J., Spaulding, J., Anwar, A., et al. (2019). IoT malware ecosystem in the wild: A glimpse into analysis and exposures. In *Proceedings of the 4th ACM/IEEE symposium on edge computing, SEC 2019* (pp. 413–418). ACM.

58. Dewi Rosadi, S., Suhardi, S., & Kristyan, S. A. (2017). Privacy challenges in the application of smart city in Indonesia. In *2017 international conference on information technology systems and innovation, ICITSI 2017 - proceedings* (pp. 405–409). Institute of Electrical and Electronics Engineers Inc.
59. Hoe, S. L. (2016). Defining a smart nation: The case of Singapore. *Journal of Information, Communication and Ethics in Society, 14*, 323–333. https://doi.org/10.1108/JICES-02-2016-0005
60. Gupta, A., Panagiotopoulos, P., & Bowen, F. (2020). An orchestration approach to smart city data ecosystems. *Technological Forecasting and Social Change, 153*, 119929. https://doi.org/10.1016/j.techfore.2020.119929
61. Angelidou, M. (2017). The role of smart city characteristics in the plans of fifteen cities. *Journal of Urban Technology, 24*, 3–28. https://doi.org/10.1080/10630732.2017.1348880
62. Rothkrantz, L. J. M. (2016). Flood control of the smart city Prague. In *2016 smart cities symposium Prague, SCSP 2016*. Institute of Electrical and Electronics Engineers Inc.