SECURITY ISSUES AND SOLUTIONS FOR SMART CITIES POWERED BY IoT

[1]Bhupendra Dhakrey, [2]Hari Om Sharan, [2]C. S. Raghuvanshi
1- Research Scholar, Rama University Uttar Pradesh, Kanpur
2- Professor, Rama University Uttar Pradesh, Kanpur
dhakrey@gmail.com

ABSTRACT:
The city has started the transition to becoming a smart city in order to draw in new people and businesses, enhance resident quality of life, manage existing resources like roads and water in an economically sustainable manner, and minimise environmental pollution. The city, its citizens, tourists, and business and private entities with a presence in the city have all benefited from the transformation to a smart city. However, due to the interconnectedness of the OT (Operational Technology) and IT (Information Technology) infrastructures, there are now cyber security vulnerabilities. However, the increased connectivity and data sharing with intelligent machines and their software come with a significant risk of IT security issues; security for emerging IoT technologies must not be a development afterthought as the future of humanity and society will depend on it. Internet of Things (IoT) technologies offer new ways for businesses and governments to create value. Both traditional methods like malware, data manipulation, and DDOS as well as a variety of cyber attack tactics including remote execution and signal jamming can be used against smart cities. This article will provide a multilayered security strategy for protecting their smart city infrastructure and the data that goes along with it.

Keywords: Information security, IoT, data protection, smart cities, smart healthcare, software vulnerabilities

DOI Number: 10.14704/nq.2022.20.13.NQ88436 **NeuroQuantology2022;20(13): 3547-3554**

INTRODUCTION:

In order to develop a comprehensive system of effective urban services, the definition of a "smart city" entails the integration of present substructure with new information and communication technology (Maruf et al., 2020). A smart city is one that combines its social infrastructure, commercial infrastructure, information technology infrastructure, and physical infrastructure to increase its collective intelligence (V et al., 2018). The enormous, intricate, and reliant technologies that make up the "smart city" face several technological, economic, political, and social problems (Al-Saidi and Zaidan, 2020). Issues and obstacles that smart cities face include those related to economics and investments, people's constantly changing needs, stakeholder cooperation, user-friendly jointing, safety and security, and others (Aghajani and Ghadimi, 2018). Cities may generally benefit from being smarter in six areas: clever people, smart governance, smart economy, smart transportation, environment, and living (Razmjoo et al., 2021). By offering relevant and effective services, smart cities met the needs of businesses, residents, and institutions. It is possible to expand urban services in a number of areas, including the environment, transportation, health, tourism, energy management, and home safety (Vitunskaite et al., 2019). Despite the advantages of creating smart cities for people, businesses, the environment, etc., these cities are vulnerable to multiple cyber-security risks, making it challenging to achieve a security maturity in them (Baig et al., 2017). In a smart city, one careless move by a person or group might endanger the entire community (Zhou et al., 2021). A significant difficulty for digital court investigations is this complicated city. In order to safeguard data and the lattice from any attacks and negative deeds in a smart city, security must be ensured (Sengan et al., 2020). The producers of the software and hardware used in smart cities rarely evaluate the cyber-security of those products. Therefore, using such security flaws could result in the system being hacked, having fraudulent data added to it, or even being stopped (Sengan et al., 2021). Cybersecurity is not the only problem; privacy protection and citizen connections with the government are also important (Chen, 2021). The usage of this technology by consumers will be questioned due to the potential for privacy invasion and the absence of cyber security in smart cities (Lim et al., 2021). Identifying cyber security issues and risks to citizen privacy is the first step in resolving issues with cyber security in smart cities and protecting citizens' privacy (El Hilali and Azougagh, 2021). One cannot expect the design, implementation, and development of a smart city to be successful without being aware of these issues and offering suitable answers (Kashef et al., 2021). On the other side, the UN estimates that by the end of 2050, there will be roughly 7.9 billion people on the planet. According to estimates, 75% of the world's population will live in cities, with some of those cities having populations of over 10 million. Deep learning is now frequently used to data that researchers have gathered. Deep learning is a form of machine learning and artificial intelligence that closely resembles the methods used by the human mind to learn a particular subject. It has various uses in the smart city (Atitallah et al., 2020). Deep learning can assist the system adapt to new environments by continuously gathering and monitoring information (Singh et al., 2020). Machine learning and neural networks both gain from the use of deep learning, a subfield of artificial intelligence. Computer vision programmes have recently significantly improved in several domains, including robotics, natural language processing, and many others, when compared to traditional machine learning techniques (Belhadi et al., 2021).

Urban regions have started to see the emergence of "smart cities" to enhance resident quality of life and increase governance effectiveness. A city's digital infrastructure is fed by a combination of street lights, traffic signals and cameras, electric and gas meters, and sewers in "smart cities." Think of connected cities as smart cities that use anything from IoT sensors to open data collecting to smart streetlights to improve communication and services (Maddox, 2016).

There are several advantages for residents, visitors, and businesses and corporate organizations situated in a smart city, including the following:

- Residents
  - ✓ A less congested and more pedestrian-friendly city
  - ✓ More effectively providing inhabitants with services
  - ✓ Greater consideration for residents' needs by the city
  - ✓ Better living conditions and a higher standard of living
- Locally based businesses and corporations

eISSN 1303-5150

        - ✓ A more crowded talent pool as a result of the increase of people opting to live in cities
- ➢ Visitors
    - ✓ Less crowded, more accessible by foot, and safer city
    - ✓ Convenience and effectiveness while utilizing city resources and services
- ➢ Cities
    - ✓ Attracting more people to the city will result in more tax revenue.
    - ✓ Elimination of redundancies
    - ✓ Simplifying the duties of employees

However, the interconnection necessary to make the idea of a smart city a reality also brings with it vast amounts of data coming from different endpoints. This information may be sensitive, personally identifying, or financial, making it a gold mine for hackers and online criminals.

Data pertaining to all types of privacy are accessible to smart cities. Additionally, the scope, level of detail, and volume of data acquired from common individuals have been dramatically increased by the technology that drives smart cities. A number of practices that are typically regarded as unacceptable but are a necessary component of operations in a smart city ecosystem have been identified as having the potential to threaten and violate privacy, according to Ernst & Young's report Cyber Security: A necessary pillar of Smart Cities.

- ➢ Surveillance: Watching, tracking, listening to or recording a person's activities
- ➢ Aggregation: Combination of various aspects of data about a person to identify a trend or pattern of activities.
- ➢ Data leakage: lack of data protection policies can lead to leakage or improper access of sensitive information.
- ➢ Extended usage: use of data collected for period longer than stated or for purposes other than the stated purpose without the subject's consent

Some of the components of smart city infrastructure that cause concern are as followed:

- ➢ Insecure hardware: It's possible that sensors in buildings, equipment, and devices are not secure or fully verified. IoT devices are currently not standardized, making sensors vulnerable to hacking. Hacking of sensors could result in signal failures and system shutdowns.
- ➢ Larger attack surface: Information and communication technology (ICT) infrastructure is a complex, networked assembly that is used by smart city operations to administer a variety of services. There are several access points, and if one device is compromised, an attack on the system or network as a whole is possible. Weak security and encryption, the use of outdated, insecure technology, poor maintenance, cascading effects, and human mistake all contribute to this vulnerability. The integration of security between IT and OT will probably provide unforeseen risks as the IoT gets closer to the centre of digital business for both the private and public sectors. Theft of sensitive information, compromise of personal private information, influence on business and city operations, and harm to vital infrastructure are just a few of these possible threats.

DATA ANALYSIS:

According to Gartner, 2.3 billion linked items will be used in smart cities this year, and 8.4 billion connected things will be in use globally in 2017. By 2020, 20 billion new IoT objects will be available. IoT deployment is fraught with problems, some of which are connected to the gathering, storing, and utilization of data obtained through the use of IoT devices. The majority of businesses and local governments lack the knowledge and resources necessary to create, implement, and run such an ecosystem on their own. Nearly 20% of firms reported having seen at least one IoT-based attack in the previous three years, according to a recent Gartner poll. As part of the 20 billion new IoT devices that will be accessible by 2020, LOB devices from vertical areas like healthcare, manufacturing, and oil and gas continue to use conventional CPUs, memory, and industry standard network connectivity. However, a lot of these devices are "headless" since they have insufficient memory and processing power, which increases the attack surface for IT. Further aggravating the issue is the convergence of building automation (BA) and industrial OT devices onto the bandwidth-intensive company and city infrastructure (Zimmerman & Pace, 2018). More than 40% of industrial control systems (ICS), which regulate physical infrastructure, were malware-infected, according to Kaspersky Labs. As an illustration, hackers were able to breach the Bowman Avenue Dam in Rye Brook, New York, in 2016 and alter the dam's controls, posing a risk of flooding hundreds of nearby homes. Transport systems appear to be at risk as well. It was discovered that about 25% of the San Francisco Municipal Transportation Agency's (SFMTA) networking infrastructure had been compromised by ransom ware. Over the 2016 Thanksgiving holiday, the malware opened the barriers, allowing customers to take free trips, resulting in significant revenue losses for the city. Another example was the 2016 hack of the Dallas city warning system. The 156 emergency sirens all began to sound, waking up the public and overtaxing the 911 operators. The attack goes beyond an annoyance since it might put lives in jeopardy by depriving the city of emergency services and using up valuable resources (ITOne, 2017).

PROBLEM STATEMENT:

IoT-based attacks are already a reality as the praised IoT expands at a startling rate. "Since Atlanta's computer systems were attacked by ransom ware, the death toll has risen. The city has requested nearly $15 million to fix its broken systems since March of this year. It lost access to more than a third of its programmes or had them at least partially disabled. Years' worth of police dashcam footage just disappeared, prompting experts to speculate whether the data leak may endanger any pending criminal cases. (PWC, 2018)

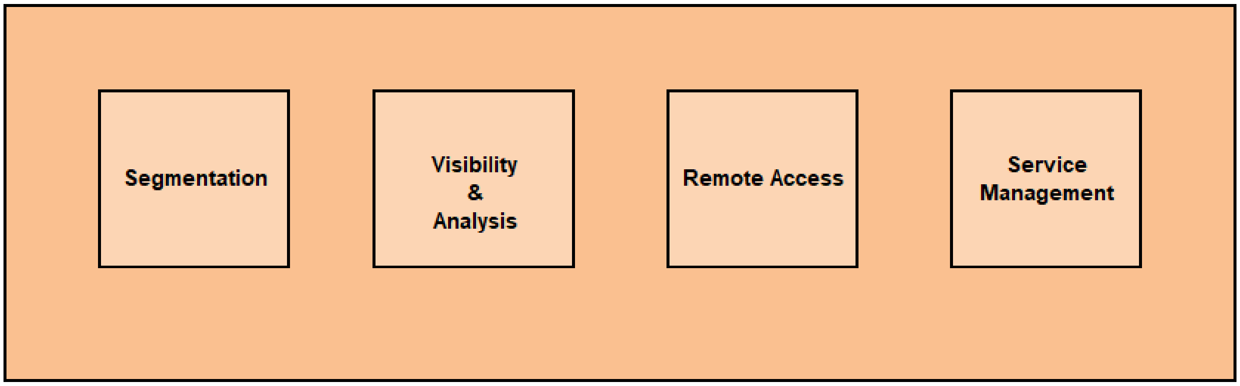
The smart city having main concerns about their IoT-enabled network infrastructure as followed:

- Historically air-gapped networks for line of business (LOB), operational technology, and building automation are convergent into the city's infrastructure, adding additional IoT devices and increasing attack opportunities.
- The weak or nonexistent authentication on new IoT devices makes it possible for unauthorized users to access city networks, expose citizen data, and incur financial losses for the city and taxpayers.
- There is no network insight over who, when, where, and with what network access the IoT devices are linked to the city's network infrastructure.
- The proxy paradigm functions effectively for managed devices. However, they become unmanageable

when the monitored devices are offline or not linked to City's corporate network. Additionally, BYOD devices lack malware detection and threat prevention mechanisms because they are not managed.

PROPOSED SOLUTION:

In order to address the threat these threats pose to the IoT-enabled digital infrastructure on four crucial fronts, we suggested IoT threat defense solutions for smart cities.



The first stage in creating a defense-in-depth architecture for a city is to link all of the threat-defeating capabilities with the operational tasks, procedures, and services provided by the city. We suggested software-defined segmentation as the first step in our IoT security solutions, followed by visibility and analysis, remote access control, and IoT network service management and automation.

SEGMENTATION:

Visibility is usually where security begins. However, segmentation comes first for IoT systems. In addition to creating a software-defined perimeter to safeguard the City's assets from known and unknown hazards on the existing network, intelligence segmentation also keeps these devices out of harm's way for new installations. As a result, if these devices are compromised, it prohibits other devices from using them as pivot points to move across the network.

Capacity Needed	Solution Functions
Identity	Identity of users and devices for access control that is context-based, taking into account factors like location, time of day, and security posture.
Profile	Profile tools Profiling defines the contextual components required for device classification and categorization when connected to the network.
TrustSec	Software-defined segmentation based on identity. Prevents unidentified IoT devices from connecting to the network and separates IoT systems and users according to role and regulation.

VISIBILITY:

Once the initial level of segmentation is in place for known IoT devices and users, adding layered defense for visibility enables identification of undocumented devices on the network. City gets control for detecting and remediating those threats as all devices become identified and known.

Capacity Needed	Solution Functions
Identity	Identity of users and devices for access control that is context-based, taking into account factors like location, time of day, and security posture.
DNS Security	Identifies Internet traffic from all connected devices using name resolution, blocks malicious sites, and disables command-and-control callbacks.
Network Monitoring	Recognizes and issues alerts on aberrant device traffic flows, and uses infrastructure communication flow statistics to help locate network annoyances.
Analysis and Detection	Establishes a baseline for city operations and known devices linked to the network by analyzing typical IoT network behaviors. When abnormal behaviors begin, it generates alarms.
Intrusion Prevention	Deep packet inspection gives IoT visibility and prevents attacks, exploitation, and information gathering.
Threat Intelligence	Provides information on current malware, communication methods, and learning information on new behavioral threats.

REMOTE ACCESS CONTROL:

Vendors must have remote access to their devices for operation and maintenance in order to sustain the City's pricey and sophisticated IoT investments. Legacy modems and other connectivity techniques, such as physical presence suppliers' usage of them in the past, are replaced by secure remote access, closing the back doors to the digitally connected network.

Capacity Needed	Solution Functions
Identity	Identity of users and devices for access control that is context-based, taking into account factors like location, time of day, and security posture.
VPN	Based on role and policies, offers remote operators, vendors, and providers secure encrypted access.
AntiMalware	Checks files for malware and viruses, promptly quarantines and removes any threat, and does so before it can infect weak IoT systems.

SERVICE MANAGEMENT:

A secure IoT network can be built with the aid of all the features mentioned above. It is vital to thoroughly study and evaluate the city's environment before implementing these. To get the highest return on investment from the City's IoT projects, we advise adding deployment and incident response services early on. Many of the solutions presented here, like the design and implementation of ISE and Stealth Watch, are challenging for the City to complete independently:

• Security penetration assessment
• Automation and control system risk assessment
• Privacy impact assessment
• Incident response services
• Software defined segmentation service

Key Advantages of Solutions:

Simplify access management

• Control access to vital assets based on departmental function, device type, and physical location.

• Manage access control and segmentation across the digital infrastructure of the city with ease.

Gain policy uniformity throughout the whole network infrastructure

• Apply regulations uniformly throughout the IoT-enabled network and scale from mobile users to the data centre and public cloud.

• Apply and enforce consistent policies centrally across users and devices with wired, wireless, and remote access.

Reduce operational expenses

• Software-defined segmentation can limit the effect of data breaches and minimise the spread of threats and compromises across the city's network.

• Reduce the need for expensive and time-consuming transfers, ads, and change management by automating the administration of firewall rules and access control lists (ACL).

• Avoid costly network redesigns and easily comply with audits to meet compliance needs.

Gain visibility across whole IoT infrastructure

• Gain visibility into all network communications in order to detect internal and external risks.

• Conduct advanced security analytics and gather in-depth information in order to detect a wide variety of unusual behaviors.

• Accelerate and enhance worldwide threat detection, incident response, and forensics.

• Enable deeper forensic investigations using network activity audit histories increasing network visibility simplifies compliance, network segmentation, performance monitoring, and capacity planning.

References:

1. Adams, R. (2016, March 25). Is Artificial Intelligence Dangerous? Forbes. Retrieved from, http://www.forbes.com/sites/robertadams/2016/03/25/is-artificial-intelligencedangerous/#630b4a171d01
2. Cybersecurity of the Internet of Things. (n.d.). Retrieved from https://oversight.house.gov/hearing/cybersecurity-internet-things/ Hearing held on October 3, 2017
3. Cisco IoT Security. (2018, September 26). Retrieved from https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html
4. (2017, June 23). Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/enterprisenetworks/trustsec/solution-overview-c22-737173.html Cisco TrustSec solution overview. Cisco TrustSec helps organizations protect their most critical assets from malware and bad intent by controlling access to your applications, equipment, and users.
5. Etherington, D., & Conger, K. (2016, October 21).
6. Large DDoS attacks cause outages at Twitter, Spotify, and other sites.

Retrieved from https://techcrunch.com/2016/10/21/many-sites-includingtwitter-and-spotify-suffering-outage/

7. Forbes, H. (n.d.). Software-defined Industrial Networks Deliver Cybersecurity Breakthroughs. Retrieved from https://www.arcweb.com/blog/software-defined-industrial-networks-delivercybersecurity-breakthroughs
8. Gupta, A. (2017, August 06). What Cyber Threats Are Smart Cities Facing? An in-depth look . . . Retrieved November 23, 2018, from https://newcities.org/the-big-picture-ai-smart-cities-privacy-trustethics
9. IoT Framework Assessment. (2016, May 14). Retrieved from https://www.owasp.org/index.php/IoT_Framework_Assessment Explores specific security related concerns of typical IoT system archetypes – gates, gateway, cloud platform and mobile.
10. IoT Threat Defense for Manufacturing SAFE Design Guide. (2018, May). Retrieved from https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zonesecurity/iot-threat-defense-mfg-design-implementation-guide.pdf.
11. Jain, H. (2016, November 24). Managing the Attack Surface of a Smart City. Retrieved from https://www.fortinet.com/blog/industry-trends/post-mirai-managing-the-attack-surfaceof-a-smart-city.html
12. JustinGopinath, N. Y. (n.d.). DDoS Mitigation using Software Defined Network. Retrieved from http://www.ijettjournal.org/2015/volume-24/number-5/IJETT-V24P246.pdf
13. Kiertzner, H. (2018, June 14). The first step in ensuring cybersecurity: Understanding what's normal. Retrieved from https://na.smartcitiescouncil.com/article/first-step-ensuring-cybersecurityunderstanding-whats-normal
14. Maddox, T. (2016, August 1). Smart Cities: 6 Essential Technologies. Retrieved November 23, 2018, from https://www.techrepublic.com/article/smart-cities-6-essential-technologies/
15. National Institute of Standards and Technology. Cyber-Physical Systems (CPS) Framework Release 1.0 (n.d.). Retrieved from https://pages.nist.gov/cpspwg/
16. Raza, K. (2016, December 01). How to architect the network so IoT devices are secure. Retrieved from https://www.networkworld.com/article/3146090/internet-of-things/how-to-architect-thenetwork-so-iot-devices-are-secure.htm
17. (Hari Om Sharan, 2022)
18. (Hari Om Sharan Umesh Kumar Gera, 2021)
19. (Hari Om Sharan C. R., 2014)
20. (Dikchha Dwivedi, 2021)
21. (Kumar, 2020)
22. (Bhupendra Dhakrey, 2022)