Introduction

Various countries classify waste management and disposal systems as critical infrastructure due to its direct implication on the health of the citizens (Novikovas and Stankevičius, 2018). A well-designed waste management system plays a vital role in allowing sustainable and ecological disposal of waste while protecting the environment. Rapid migration of population to urban area are challenging the city infrastructure and are demanding for more scalable solutions that are deemed to be more dynamic, economic, reliable, sustainable, and transparent. Detailed study and experience from designing smart cities identifies IoT technology as a credible solution (Fazio et al., 2012).

A sophisticated IoT solution can not only fulfil all the above requirements but could be integrated with the current waste management systems with minimal disturbance.

But introduction IoT based solutions increases the attack surface considerably due to the number of devices that are required to be connected to the infrastructure. Cybercriminals have been increasingly targeting IoT devices and gadgets in recent years primarily due to spread of devices involved, constrained requirement that limited power supply, processing capabilities. Moreover, recurrent duty cycles needed for charging, firmware upgrade and uncontrollable product development life cycles of the equipment manufacturers (Coker, 2021).

Any manipulation in even one of these widespread devices will compromise the security of the whole network infrastructure it is connected to. Cyber-attack on waste management can disrupt the daily routine of the citizens and even cause environmental hazard in the form of cross contamination of waste, various types of pollution. Furthermore, a compromised IoT based waste management can leak personal information that can be used for social engineering attacks.

Hence, Government of UK as formally passed The Product Security and Telecommunications Infrastructure (PSTI) Bill, which in turn enforces implementation of security in waste management systems.

Research Problem

Lack of understanding of the risks these technologies bring at the community level owing to.

1. The increased attack se attack surface due to the number of devices required.
2. Limited processing power and resources available on the sensors (battery, charge, processing)
3. Nonnegotiable requirement of uninterrupted connectivity to the command-and-control center.
4. Provisions for manual override in case of malfunction or hacking.
5. Difficult to service/upgrade once deployed.

Hence, we propose to test a prospective taxonomy that identifies areas to exercise idea of "security by design", by inculcating security in very phases of waste management system.

1. Collection
2. Transportation
3. Disposal.

Research Question

Our research question focuses on "How can we introduce an added layer of security to the existing infrastructure of IoT based waste management systems while considering the real-world challenges that can influence their implementation?"

Without increasing the number of devices or security overheads for the people on the ground.

Literature review

Speed of urbanisation has forced smart device industry to focus on optimizing efficiency, durability, production costs and meet the foreseeable volumes of IoT devices. The generic sensors including infrared sensors, thermometer, barometer, lidar can be used in multiple configurations and settings. The smart sensors interconnect with telecommunication infrastructure to transmit the reports, data and flag events like acknowledgment, anomalies, etc. The use cases can range from waste identification before collection to confirmation of incineration. Smart bin can signal the local authorities to indicate when they are more than 80% - 90% full and will soon require collection (Pankaj et al., 2015). The Rao et al. in their model propose monitoring of the smart bin levels achieved by ultrasonic sensors and information is transmitted wirelessly, the over the internet using Blynk platform which helps in achieving real time access of data(Rao et al., 2020). Data collected from these smart devices will allow in better understanding of the trends to help us improve the reliability of the system and scale in the later phases of rollout. The IoT based waste management using smart bins is an evolving technique that will help keep local authorities clean & healthy. Similarly for transportation with the use of weight sensor, fume detectors we can monitor the garbage, in transit. Cyber-attacks targeting the critical infrastructure can directly impact the routine functioning of the society, ecological health, data privacy and worst even human life.

Author (Alladi et al., 2020) emphasizes the danger and potential risks posed by an IoT device & further its counter measures:

1. Device Software Failure: In this form of attack any underlying vulnerability in the device's software can be exploited.

countermeasure: regular software updates/patches (Kaspersky Lab Security Services., 2018)

2. Node Tampering Attack: in this attack, attacker gets the hold of physical device and tampers with its electronic circuit manually.

   Tamper-resistant hardware primitives such as physically unclonable functions (PUFs) can be added to the chip. (Kumar et al., 2019)

3. Eavesdropping Attack also known as snooping attack, where theft of information occurs while network traffic flowing from an intended IoT device.

   Enabling encrypted communication to establish the privacy of other devices on the IoT network.

4. Malicious Code Injection: in this attack, malicious code is injected in the IoT device through the firmware/software vulnerability.

   Appropriate authentication mechanisms should be implemented from the beginning of the code's execution (Arias et al., 2015).

5. Unauthorized Access: in an iOT device by exploiting both software & hardware vulnerabilities & carrying out brute force attack an attacker can acquire unauthorized access

   Produce session keys, Randomizer should be used in place of static secure tokens.

6. Social Engineering Attack: it's a kind of attack that largely relies on individuals personal & sensitive information.

   Use multifactor authentication and avoid sharing any personal information including birthdates, birthplace etc.

Anagnostopoulos in his comprehensive survey studies the various waste management systems and smart devices in their respective settings (Anagnostopoulos et al., 2017). The survey proposed a fundamental classification that delineates the scope of:

1. Physical infrastructure
2. IoT Technology
3. Software analytics

This taxonomy served as a great starting point to comprehend the roles and responsibilities of the various devices. However, it wasn't enough to identify possible gaps in the security realms. Hence identification of gaps required careful consideration the phases and steps involved in waste management systems from a security standpoint while considering real-world challenges.

Research Methodology

The research methodology is divided into 6 distinct parts, namely:

1. Collaboration
2. Analysis
3. Designing & Planning
4. Development & Testing
5. Trials & Survey
6. Feedback analysis and Dissemination

In London, Mayor decides strategies for waste management system but rely on the local authorities for waste management processes.

The local authorities are responsible for the processing of the collected waste from households, industries, commercial sites. Hence, we choose to collaborate with the local authorities to understand the existing processes. This step helps in the analysis of their requirements while considering the best practices documented in the smart city studies.

We us the collected data to construct model and evaluate feasibility statistically and start with the solution designing and planning. Planning is accompanied by development and integration of prototypes which are tested against the requirements. After successful testing the solution will be offered for user trails for the operators followed by a detailed survey.

The survey along with chosen performance indicators will determine the success of the proposed taxonomy.

Significance of our Research

When it comes to the environment, waste management tops the list, making it one of the most pressing issues to handle. Moving forward in the digital age, security is something that cannot be overlooked.

Security and environment are the terms we rarely hear together. So, what do they both have in common? Well, there's a lot more to it than meets the eye. It is at the infrastructure level where the main cyber security threat exist. As previously mentioned, waste management is divided into three phases, each of which necessitates the use of smart bins and a collection network. All of this is infrastructure intensive and is all linked through command-and-control centres (C&C). Each center is run by a network of computers that are linked together, which in turn are vulnerable to a variety of security risks covering both ends of the spectrum from intrusion attacks to internal bad actors. This entire paradigm makes security a major concern for reliable waste management systems.

Bear in mind the increase in medical waste over the last two years, as well as its collection and disposal, it has become even more vital for the human population. As a result, a cybersecurity failure could pose a significant health risk. Hence, any security breach that jeopardizes public health would cost far more than just physical damage.

The model is built on the interrelationships of major factors affecting the collection, transportation and disposal.

Our model's proposed advantages are as follows:

1. Ensures that all sites' areas are secure against Malicious Users or Waste Thieves.
2. Control access to the site for both personnel and visitors.
3. Monitor security cameras and intruder alerts.
4. Identification of trespassing incidents.
5. Transparency & Back-traceability from source to disposal.
6. Multi-Level authentication not only for the devices but also the vehicles involved in the process of transportation.

Proposed taxonomy & artefacts

Performance indicator of proposed taxonomy include:

1. User Security
2. Device/Sensor Security
3. Traceability
4. Re-use sensors to decrease e-waste
5. Seamless integration with infrastructure
6. Version Control for vulnerability tracking
7. Battery power overheads

We achieve logical separation of the sensors, users, roles with distinct read-write capabilities. Use multifactor authentication to provide role-based access for operational tasks like monitoring, data collection, data collection and logs. Manual check and override mechanisms to enforce physical security of the operators, devices/equipment and citizen. Strict procedures to have version control and firmware. Use of IoT Technology will not only help us making waste management secure but also allow us to measure the ecological sustainability goals. While in transit the command-and-control center can monitor the activities of the vehicles carrying waste. The operators can monitor temperature, smoke, fumes and leaks to identify spillage. In case of heavy machinery and fire the provision of manual check give the ability override the physical system. In case non-conformity the user will be denied the access to commit any actions.

References

Alladi, T., Chamola, V., Sikdar, B. and Choo, K.-K.R. (2020). Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine, [online] 9(2), pp.17–25. Available at: https://ieeexplore.ieee.org/abstract/document/8977812/figures#figures [Accessed 3 Apr. 2022].

Anagnostopoulos, T., Zaslavsy, A., Medvedev, A. and Khoruzhnicov, S. (2015). Top -- k Query Based Dynamic Scheduling for IoT-enabled Smart City Waste Collection. 2015 16th IEEE International Conference on Mobile Data Management. [online] Available at: https://ieeexplore.ieee.org/abstract/document/7264372 [Accessed 23 Mar. 2022].

Anagnostopoulos, T., Zaslavsky, A. and Medvedev, A. (2015). Robust waste collection exploiting cost efficiency of IoT potentiality in Smart Cities. 2015 International Conference on Recent Advances in Internet of Things (RIoT). [online] Available at: https://ieeexplore.ieee.org/abstract/document/7104901 [Accessed 23 Mar. 2022].

Arias, O., Wurm, J., Hoang, K. and Jin, Y. (2015). Privacy and Security in Internet of Things and Wearable Devices. IEEE Transactions on Multi-Scale Computing Systems, [online] 1(2), pp.99–109. Available at: https://ieeexplore.ieee.org/abstract/document/7321811 [Accessed 3 Apr. 2022].

Novikovas, A. and Stankevičius, A. (2018). MUNICIPAL WASTE, AS CRITICAL INFRASTRUCTURE, MANAGEMENT: CASE OF LITHUANIA. *Journal of Security and Sustainability Issues*, 8(2), pp.135–143.

Kumar, S.K., Satheesh, N., Mahapatra, A., Sahoo, S. and Mahapatra, K.K. (2019). Physical Unclonable Functions for On-Chip Instrumentation: Enhancing the Security of the Internal Joint Test Action Group Network. IEEE Consumer Electronics Magazine, [online] 8(4), pp.62–66. Available at: https://ieeexplore.ieee.org/abstract/document/8732719 [Accessed 3 Apr. 2022]

Kaspersky Lab Security Services", 2018, [online] Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/ 12/13084354/ChargePoint-Home-security-research_final.pdf. Pankaj Morajkar, Vikrant Bhor, Pandya, D., Deshpande, A. and Maheshwar Gurav (2015). Smart Garbage Management System. International Journal of Engineering Research & Technology, [online] 4(3). Available at: https://www.ijert.org/smart-garbage-management-system [Accessed 4 Apr. 2022].

Rao, P.V., Azeez, P.M.A., Peri, S.S., Kumar, V., Devi, R.S., Rengarajan, A., Thenmozhi, K. and Praveenkumar., P. (2020). IoT based Waste Management for Smart Cities. 2020 International Conference on Computer Communication and Informatics (ICCCI). [online] Available at: https://ieeexplore.ieee.org/abstract/document/9104069 [Accessed 3 Apr. 2022]