Surveying Cyber Attacks in Smart Cities and DDoS Mitigation Strategies

Ilavendhan[1], Jayanthi Sharma[2] and Kashish Mahendra[3]
[1]Assistant Professor, School of Computer Science and Engineering
Vellore Institute of Technology, Chennai, India
Ilavendhana62@pec.edu, Mobile: +979017696
UG Scholar, School of Computer Science and Engineering
Vellore Institute of Technology, Chennai, India
[2]jayanthi.sharma2022@vitstudent.ac.in, Mobile: +918618556742
[3] kashish.mahendra2022@vitstudent.ac.in, Mobile: +918837696221

Abstract: As urban centers increasingly embrace connectivity, the rise of smart cities offers a promising avenue to tackle urban challenges. However, the surge in data generated by smart city infrastructure has sparked concerns about data security, privacy, and efficiency. This paper delves into the current status of data security attacks and the countermeasures within smart cities. It surveys the existing as well as the potential solutions to such issues and weighs them against various measures such as feasibility, efficiency, and implementation.

It starts by examining the existing data security issues encountered by smart cities, emphasizing the vulnerabilities of conventional attack prevention methods and the growing risk of cyber threats. Furthermore, it outlines the constraints of present data transmission technologies and presents the limitations of known approaches.

The paper suggests a multifaceted approach to effectively mitigate DDoS attacks in smart cities. We propose a comprehensive solution that integrates a permissioned blockchain network, lightweight agents for anomaly detection, quantum-enhanced traffic analysis, and a reputation-scoring system.

Keywords: Smart City, Data Security, Data Transmission, Cyber Attack, Encryption, Adoption barriers, DDoS, Permissioned-blockchain, Lightweight Agents, Quantum.

1 Introduction

In recent years, there has been a growing global interest in the concept of smart cities - urban environments that leverage cutting-edge technology and data-driven solutions to improve the quality of life for their residents. A smart city is a technologically enhanced city that not only improves the quality of life of the citizens residing in it but also supports sustainable development by harnessing the resources efficiently and judiciously. These cities aim to enhance efficiency, sustainability, and livability by integrating various aspects of urban life, such as transportation, energy, governance, and public services, into a seamlessly connected ecosystem. From a technical viewpoint, the smart city may be conceptualized as a framework that translates the physical and behavioral attributes of various city elements (including citizens, services, and physical infrastructure) into the digital realm. This translation is facilitated through the interoperability of technological subsystems composed of sensors, actuators, and processing capacities [1]. The potential advantages of smart cities are diverse and encompass a range of benefits that resonate across urban society [2]. As smart city developments propel forward to enhance the quality of life and drive sustainable development, they encounter a myriad of challenges. While these urban environments promise improved efficiency, connectivity, and resource management, issues such as socioeconomic disparities, digital divides, and environmental sustainability remain significant hurdles.

By 2024, the number of smart infrastructures for digital urban services is estimated to be around 1.3 billion [3]. According to the United Nations Population Fund, around 3.3 billion people—or 54% of the world's population—lived in urban areas in 2014; this figure is expected to rise to 5 billion (i.e., 66%) by 2030. If urbanization continues at this rate, it will have a severe impact on city management, security, and the environment. To effectively manage data analysis, data communications, and the successful execution of complicated strategies to maintain the smooth and secure functioning of a smart city, the efficient use of ICTs is very important [4-6].

While smart cities encounter numerous challenges during their development, including socioeconomic and political issues, the primary obstacle lies in technical issues. Within the realm of technical challenges, alongside concerns such as system interoperability and cost-effective technology, the importance of addressing security and privacy cannot be overstated [7]. The realm of information security primarily addresses the security and privacy concerns associated with data. It aims to shield information from various threats, including attacks, viruses, frauds, and other malicious activities that could compromise both the integrity of the data and the demand for information within technologically integrated smart cities. Security holds significant importance in smart city infrastructures due to the susceptibility of networks to a broad spectrum of malicious attacks. Given the lack of trust in both internal and external parties, ensuring robust security measures is essential for garnering consumer acceptance [8]. Incorporating security protocols to protect data, digital infrastructure, and citizen privacy is fundamental for the sustainable and effective implementation of smart city projects [9].

To make the idea of a smart city a reality, a crucial requirement is that all the critical sectors like transportation, communication, healthcare, education etc. must be well-connected and secure. Since smart cities are technology-based, it is natural to expect attempts of security breaches. This proves to be a major concern for the protection of data. Over the years, various data security techniques have been implemented to tackle such problems, yet no solution is successful in its entirety.

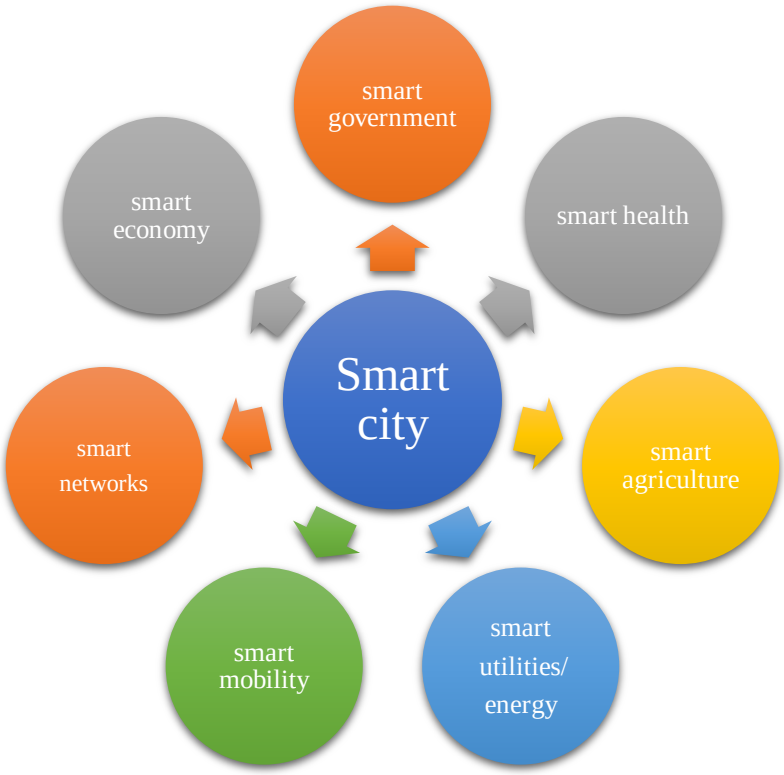

Fig. 1. Smart City components

In chapter two, we delve into the various cybersecurity challenges and threats associated with the implementation of smart technologies in a smart city environment. We explore various types of cyber attacks and their classification and have included a survey of recent cyber attacks on smart cities.

Chapter three examines various existing research papers that offer insights and solutions to counter these cybersecurity threats. In chapter four, we discuss DDoS attack and the threat it poses by analyzing the recent DDoS attacks. Further, chapter five includes the proposed work of a permissioned blockchain network involving shared evidence, reputation scoring, and traffic analysis agent. Chapter six mentions the implementation methods for the proposed model. Chapter seven discusses the challenges in implementation of DDoS mitigating startegies. Finally, we have suggested the future work in this domain.

2 DATA SECURITY CHALLENGES:

Every new smart technology used to secure a smart city creates a potential opportunity for a cyber attacker to intrude. There can be devastating effects on entire nations if data security is overlooked. Consider the data Aadhar card data breach, possibly **the biggest data breach in Indian history**, that exposed the personal data of 81.5 crore Indians on sale on the dark web due to security vulnerabilities (in the year 2023) [10].

Additionally, consider the unencrypted and non-authenticated communication channels between traffic control systems and traffic lights in intelligent traffic control systems. Unencrypted and non-authenticated communication channels in intelligent traffic control systems can pose security risks, as they may allow unauthorized access and manipulation of traffic signals. Another significant threat to customer privacy arises from the possibility of malicious individuals eavesdropping on consumer data transmitted from a smart building to a smart meter. Moreover, an attacker's ability to impersonate a customer and gain remote control over building equipment can result in various detrimental consequences for the customer.

Even a critical attack on the smart grid involves causing a denial of service by overwhelming channels with congestion or flooding low-powered equipment like smart meters with excessive computational demands can lead to widespread shutdowns [11].

Since IoT services function through network protocols like DNS, HTTP, and MQTT, attackers aim to capitalize on vulnerabilities within these protocols by employing tactics such as polymorphic code, DNS Spoofing, DNS cache poisoning, Denial of Service (DoS), Distributed DoS (DDoS), and URL interpretation[12]. They can also achieve successful login access via Telnet. Upon achieving this objective, they can proceed to create shellcodes or download script files containing commands [13].

In recent times, Microsoft Azure, Google Cloud, or Amazon AWS have become the most recognized cloud forms in the field owing to their easy integration with IoT solutions. However, despite being robust commercial solutions, they expand the surface of cybersecurity attacks. Cloud solutions operate under a shared security management model: cloud companies are accountable for securing infrastructure, storage, and cloud networks, while users or clients are responsible for aspects like authentication, authorization, and continuous monitoring.

In August 2019, there was an attack in which customer data was stolen from a bank's cloud infrastructure. It was said that a misconfiguration error at the application layer caused the problem allowing a Server-Side Request Forgery (SSRF) attack. However, the judicial process investigation revealed that there were default configurations that could enable this type of attack [14].

To mitigate some of these risks, it becomes important to implement measures such as encryption and authentication which secure the communication channels.

2.1 Cyber Attacks

Cyberattacks on smart city applications can compromise their security and can be categorized into two main types: active and passive attacks.

Passive attacks aim to gather information from the system without making any changes to its resources. The primary target of these attacks is the transmitted information, with the intention of understanding the system's configuration,

behavior, and architecture. They are difficult to detect because they do not modify the data. On the other hand, active attacks are designed to cause changes or disruptions in the system's operation by modifying data or introducing incorrect information. Sabotage, manipulation, and espionage are the main motivations behind cyberattacks [15].

The cyber-attacks are also classified based on legal classification [16], they are cybercrime, Cyber espionage, Cyber terrorism, and Cyberwar.

Flowchart on Cyber Attack Classification

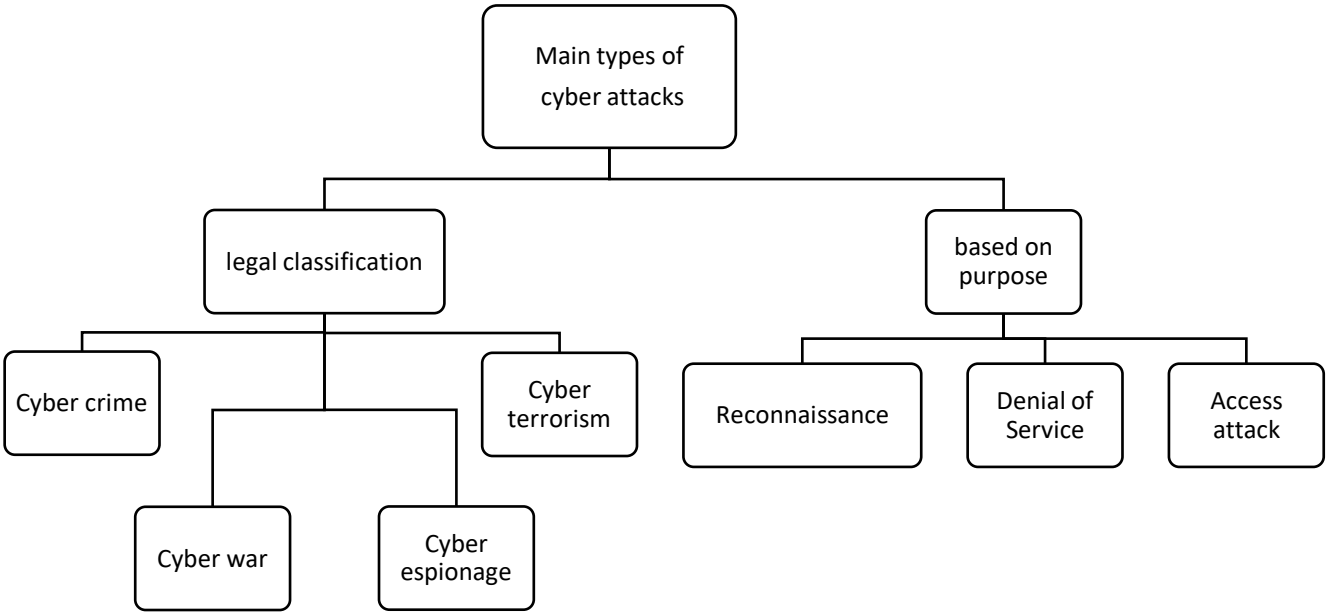

Fig. 2. Cyberattacks classification

2.1.1 Legal Classifications

Cybercrime denotes unlawful actions conducted through computers or the internet, encompassing activities like hacking, identity theft, fraud, and malware dissemination. Perpetrators typically aim at individuals, corporations, and governmental entities to illicitly access sensitive data or inflict harm. The repercussions of cybercrime can be substantial, resulting in financial setbacks, harm to reputation, and the compromise of personal or organizational information.

Cyber espionage, also known as cyber spying, encompasses efforts by unauthorized entities to access sensitive or classified information for economic, competitive, or political reasons via cyber attacks. Perpetrators may range from nation-states to terrorist groups or non-state actors. The main goal is to gather intelligence and acquire valuable data from targeted entities, leading to potential disruptions in public services, infrastructure, and even loss of life [17].

Cyber terrorism utilizes cyber attacks to instill fear, panic, or disruption for ideological, political, or religious motives. Perpetrated by individuals or groups, its aim is to harm civilians, governments, or organizations. Targets may include critical infrastructure, financial systems, or public services, with the objective of destabilizing societies and economies. The repercussions of cyber terrorism are substantial, resulting in widespread disruption, economic losses, and compromised security [18].

Cyber war denotes the employment of cyber attacks by nation-states or other entities to disrupt or harm the computer systems and networks of their opponents. It entails targeting critical infrastructure, military systems, or government networks intentionally. Cyber war can lead to severe outcomes such as service disruption, economic harm, and jeopardized national security. Attributing cyber attacks within the realm of cyber war presents challenges, as assailants frequently seek anonymity or disguise their origins.

2.1.2 Based on purpose

A Denial of Service (DoS) attack targets the regular operation of a computer system, network, or service by flooding it with traffic or requests, rendering it inaccessible to authorized users. Various methods like rate limiting, traffic filtering, and load balancing can mitigate these attacks. Quantum technology offers faster and more efficient algorithms for traffic analysis and filtering, potentially enhancing the effectiveness of these mitigation techniques [19].

Reconnaissance attacks entail collecting data on a target system or network to pinpoint weaknesses and possible entry avenues for subsequent attacks. Quantum technology aids in defending against such attacks through the implementation of robust encryption algorithms and secure communication protocols. Quantum key distribution (QKD) facilitates secure encryption key exchange, complicating attackers' attempts to intercept and decode sensitive information.

Access attacks involve unauthorized attempts to access user accounts or network devices through improper methods. These attacks, categorized as logical or physical access attacks, manifest in diverse forms.

Logical access attacks exploit weaknesses in authentication processes to obtain unauthorized entry. For instance, brute force attacks involve trying multiple password combinations, while dictionary attacks use precomputed lists of commonly used passwords to guess the correct one. These unauthorized attempts create substantial network traffic and can be identified through network monitoring systems.

Physical access attacks occur when an intruder obtains physical access to the targeted computer system or network infrastructure. This could entail directly connecting foreign hardware to the network or manipulating the system itself. Detecting and preventing physical access attacks is more difficult as they often involve social engineering tactics or physical proximity to the target.

Table. 2: Survey Table on recent cyber-attacks in smart cities

Ref. No	Smart city	Attack type	Records/attacks	Description	Year
[20]	New York	Data leak, Cybercrime	leak contains 8,761 documents most of whose deeply	Largest Data Leak In CIA's History	2017

			technical content is redacted.		
[21]	Barcelona	Ransomware attack	150 surgeries, up to 3,000 appointments and 400 canceled.	Ransomware Attack on Barcelona Hospital Threatened Urgent Care Cases, Locked Up Patient Records	2020
[22]	Tokyo	Emotet malware, email spoofing, and phishing	450 million attacks	450 million cyberattacks attempted on Tokyo Olympics infrastructure	2021
[23]	Singapore	Phishing	8500 targeted	Increase in the phishing and ransomware attacks.	2022
[24]	Barcelona	Hack, Scam, third-party fraud	5.7 million monthly visitors	FC Barcelona, Europe's top football club 's official website used by scammers in third-party fraud	2022
[25]	Singapore	Hack	40,000 targeted	Hacker steals retailer Cortina Watch's data, including customer details	2023
[26]	Dubai	Data leak	200,000 data leaked	Dubai Taxi Company, a subsidiary of Dubai's Roads and Transport Authority, leaked a trove of sensitive information from the DTC app,	2023
[27]	London	Data breach	revealed details of over 265 Afghans who were seeking relocation to Britain after the Taliban took control of Afghanistan.	UK Defence Ministry fined for Afghan data breach during Taliban takeover	2023
[28]	London	Data breach	47,000 London Met Police Officers and Staff data exposed	data breach that leaked the personal information of law enforcement officers and staff, potentially exposing the identity of undercover agents.	2023

3 Literature review

In our previous discussions, we explored various cybersecurity threats that threaten smart cities. This literature review aims to examine existing research papers that offer insights and solutions to counter these threats. By analyzing these papers, we aim to identify effective strategies and gaps in current approaches to strengthen cyber defenses.

[29] suggests the implementation of blockchain and approaches to implement a control access system that integrates the same. The escalating pace of data expansion in information gathering poses ongoing threats to our privacy. Embracing blockchain technology within Smart Cities offers a promising avenue for mitigating these privacy risks, ensuring trusted transactions, and enhancing data management. This aims to validate citizen identities, operations, and privacy safeguards effectively. Traditional access control methods are vulnerable to physical security breaches, infrastructure hacking, and unauthorized access, posing significant concerns. Numerous methods were adopted to enhance access control, such as role-based access control (RBAC), attribute-based access control (ABAC), and capability-based access control.

[30] discusses the threats of jamming attacks which is a type of Denial-of-Service(DoS) attack and regards it as one of the most severe attacks that can incapacitate IoT networks by interfering with communication channels. This is done by decreasing signal-to-noise ratio, that is, by inducing noise. To enhance the impact of the attack, these compromised nodes strategically regroup, exchange network information they've gathered, designate roles for each node as jammers and collectively achieve a more potent jamming effect. The NS-3 simulator was employed to test and propose a strategy. The experiments involved 100 valid nodes on the attack surface and examined different jammer coalition sizes (10 and 25). The results demonstrated that as the number of attacking nodes in the coalition increased, the effectiveness of the attack also increased. A comparison could be easily made between the quantity of attacks generated and the quantity of successful attacks.

Another type of attack that targets IoT devices is the Botnet Attack. Botnet attacks commonly entail activities such as data theft, the dissemination of extensive spam and phishing emails, or the initiation of large-scale Distributed Denial of Service (DDoS) attacks. They execute in multiphases.[31] proposes a two-fold machine learning approach to prevent and detect IoT botnet attacks. In the first fold ResNet-18 model was used to detect attacks in premature attack stages whereas in the second fold another model was trained for DDoS attack identification. Experiments were run on various test scenarios in which DDoS traffic was scanned from datasets. It was found that the models trained using the proposed approach gave reliable performance as compared to models directly tested over unknown datasets.

It becomes imperative to analyze the attacks carried out by intruders in order to propose new and better technological solutions. [32] presents one such approach where attacks have been assessed based on metrics namely lower and upper time bound (in days) required to achieve an attack, the cost of resources to do so as well as the probability of success. After collecting quantitative metrics of existing attacks and countermeasures, an Attack-Defense-Tree was used for modeling and risk analysis. A security configuration for IoT infrastructure is created by finding the right balance between defenses and their impact on the cost of attacks. However, only a limited number of attacks were assessed.

[33] Proposes a framework to prevent IoT devices from becoming attack targets or sources of attacks. The concept of IoT-sphere has been introduced wherein the communication boundary of IoT devices is defined. The sphere contains IPs that can communicate with a device without any violation. In case of violation, communication is halted at the gateway level. Then permitted communication was tested against potential attacks using advanced detection engines. By limiting the communication that reaches IoT devices to only what is necessary, this method allows for the conservation of the devices' constrained resources. Additionally, it lessens the workload for threat detection engines, which will improve system performance in general.

[34] has categorized attacks based on the distinct components within IoT infrastructure such as IoT devices and their peripherals, Gateways along with their internal networks, and Cloud servers and their control devices. It discusses attacks such as Sybil attacks, rolling code attacks, brute force attacks, and Buffer overflow attacks. These affect the

components in direct connection with the data collection infrastructure of IoT. The Gateway and internal network of the gateway suffer from attacks such as DNS poisoning attacks, Wormhole attacks, Replay attacks Injection attacks, and MITM attacks. Control devices and the servers of the cloud may experience Back doors and exploits attacks, SQL injection, Weak authentication, and DDoS attacks. Basic and direct measures have been listed to prevent against the mentioned attacks.

[35] a novel method for managing cybersecurity risks in smart cities, incorporating object typing, data mining, and quantitative risk assessment is proposed. It evaluates cybersecurity risks within dynamic device-to-device networks in smart cities, emphasizing threats to IoT/IIoT, VANET, and WSN inter-device infrastructures. The authors employ expert-based risk assessment, scenario analysis, functional analysis, and statistical risk evaluation methods. They propose a new approach using artificial neural networks (ANNs) for cybersecurity risk management, achieving a test accuracy of 98–99%. Traditional cybersecurity risk assessment methods are deemed inadequate for the complex digital environment of smart cities. The ANN-based approach demonstrates high accuracy in classifying big data and allows for dynamic risk assessment, even with limited awareness of the entire smart city network. Despite the need for substantial computing power and real-time data collection, the ANN-based method shows promise as a flexible cybersecurity risk assessment approach in smart city infrastructures.

[36] delves into security and privacy challenges in Smart Cities. It proposes a model depicting interactions among people, servers, and devices to ensure safety and privacy. The study highlights the evolution of Smart Cities driven by IT innovations, emphasizing interconnected systems like smart energy meters and security devices. It underscores security and privacy challenges, including illegal access and loss of privacy as citizens' data becomes more available. The authors use IBM's IN3 paradigm to analyze Smart Cities' data environment, focusing on Instrumented, Interconnected, and Intelligent aspects. They categorize information and interactions across various domains, emphasizing the need to safeguard interaction vertices and address security and privacy concerns, particularly within the U.S. automobile transportation system. The research suggests that while the benefits of Smart Cities may outweigh risks, protection of democratic rights and liberties is crucial. However, it stresses the necessity of a clear legal theory to govern the use of power represented by these systems.

Other than this, cryptography plays a crucial role in concealing data that is transmitted between users or institutions. Cryptography is the technique of securing and disguising data such that only the intended receiver will be able to unmask the received data.

A good implementation will not only improve user privacy, confidentiality and authenticity but it will also make cryptography more robust and secure. Various types of cryptographic attacks pose threats to encrypted data and communication. A brute force attack involves attempting multiple private keys until the correct one is found to decrypt the message or data. In a man-in-the-middle attack, a cybercriminal intercepts communication between two parties, potentially tampering with or eavesdropping on private information. Known plain text attacks utilize gathered information to deduce portions of the ciphertext's plaintext, helping to analyze patterns and determine the encryption key. Chosen plaintext attacks involve selecting plaintext data to acquire the corresponding ciphertext, simplifying the process of resolving the encryption key. Similarly, chosen ciphertext attacks entail analyzing chosen ciphertext to deduce secret keys or algorithm details, exploiting the relationship between ciphertext and plaintext. Differential cryptanalysis is a statistical attack that leverages encryption algorithm characteristics to deduce keys or plaintext. These various attacks highlight the importance of robust encryption methods to safeguard sensitive information from cyber threats [37].

[38] Has proposed a next-generation lightweight Cryptography (LWC) algorithm for smart IoT devices, in particular interest is laid in the performance of Long-Range Wide Area Networks (LoRaWAN), an open standard that defines

the communication protocol for Low-Power Wide Area Networks (LPWAN) technology. It was found that LWC would lead to reduced on-board memory usage and computational resource requirements, making it a more cost-effective solution that also contributes to environmentally friendly practices through power-saving measures.

Wireless Sensor Networks are another important aspect of a smart city.

A Wireless Sensor Network (WSN) is a group of spatially dispersed sensor nodes(devices), which are interconnected by using wireless communication [39]. They are autonomous and can be used to monitor environmental conditions such as temperature, pollutants, sound, etc. at different locations. A smart city highly relies on such technology owing to its cost-effectiveness and ease of deployment. Thus, it becomes imperative to understand the attacks that WSNs may be subject to. The attacks on WSN are Cryptography and non-cryptography-related attacks and attacks based on the Network Layers [40]. Some well-known attacks are Pseudorandom number attacks, Digital signature Attacks, and Hash collision attacks [41].

[42] The paper presents a hierarchical security framework designed to enhance the security of wireless sensor networks (WSNs) in smart cities. This framework incorporates usage control (UCON) and chance discovery technologies to effectively counter ongoing attacks through advanced persistent threat detection. Additionally, it employs a dynamic adaptive chance discovery mechanism to identify unknown attacks. The framework also leverages software-defined networking and network function virtualization technologies for attack mitigation. The proposed scheme's feasibility and efficiency has been validated through an attack experiment and simulations.

[43] proposes an approach wherein, the network is split into different Autonomous Systems (AS), each managing host connections. Blockchains are employed to maintain and distribute a record of Internet Protocol (IP) addresses belonging to hosts within each AS, identifying those flagged as malicious. Every AS monitors internal network communication using this approach and assesses whether a host might be infected with malware by comparing its total packet transmission with a predefined threshold.

However,it was found that the propagation delay increased with the increasing blockchain blocks.

The proposal in [44] suggests employing blockchain technology to safeguard IoT devices from DDoS attacks at the application layer by verifying and authenticating them. It also recommends tracking and storing the IP addresses of malicious devices within the blockchain to hinder their access and communication with IoT networks. The system's performance was assessed through 100 experiments.

It still needs to be evolved for countering and averting network layer attacks in order to enhance security in IoT technology. Furthermore, the system's implementation utilizing a public blockchain faces challenges related to scalability limitations.

[45] introduced an artificial immune system (AIS) as an alternative to signature-based methods to address their limitations. This approach employs the immune cell concept to develop detectors based on attack signatures, distinguishing between legitimate and malicious packets by categorizing them as self or non-self elements. The system is adaptable and can learn new patterns through continuous monitoring.

A shortcoming in this approach is that the resources in IoT networks are usually limited .This detection technique may fall short due to this.

To tackle the challenge of incentivizing cooperation and building reputation among participants in multi-domain DDoS mitigation systems[46] proposes the implementation of reward mechanisms to encourage collaboration among service providers and consumers. The paper introduces the design, execution, and assessment of a reputation scheme known as the Blockchain Signaling System (BloSS). Through automated processes facilitated by smart contracts, this system aims to identify and reward trustworthy participants, thereby deterring malicious activities. The Beta reputation metric plays a significant role in identifying and incentivizing honest contributors.

[47] introduces the use of multi-head attention mechanism to extract high-order flow-level features, reducing parameters and enhancing running time.It presents MATEC, a lightweight model for online encrypted traffic classification which operates without feature engineering or subproblem partitioning, utilizing only three consecutive packets as input and efficiently extracting high-order flow-level and packet-level features. . It significantly reduces the number of parameters to 1.8% of existing models, halving training time.

Sl. No	Objective	Attacks discussed	Methodology/proposed work	Limitations	metrics
1	Aims to propose implementing a control access system integrating Blockchain, and we discuss benefits and challenges briefly.	Hacking activities, unauthorized hacking, infrastructure hacking, cyber-attacks, privacy attacks	Paper explores the explore the benefits of Blockchain for Cybersecurity and introduces a use case of Cybersecurity in a smart building using traditional solutions and Blockchain-enabled ones to discuss the benefits, implementation challenges, and impact on resiliency improvement.	Lack of practical implementation, assumption of widespread adoption of blockchain, limited scope	
2	Presents several scenarios of a smart jamming attack (coalition attack) mechanism on IoT networks	DoSl attack black-hole attack continuous, random, deceptive, and reactionary jamming attacks	A NS-3 simulator was used to put the strategy into practice and the following were proposed: Impact of jamming attack, Comparison between number of generated attacks and number of success attacks, Transmission rate capture probability VS number of observations, False positive rate	Mechanism tested on only 25 nodes, need to scale the model up to hundreds of nodes in the future.	
3	Two-fold ML approach to prevent and detect IoT Botnet attacks	Botnet and DDoS	Several experiments were carried out to authenticate the proposed ResNetScan-1 and ResNetScan-2 model. It was proved that both proposed model outperformed all other models for detecting the scan and DDoS attacks and had a large attack pattern coverage	Only 33 types of scanning and 60 types of DDoS attacks covered.	Accuracy, precision, recsll, F1score of different models: ResNetDDoS-1: 98.70, 97.53 97.96, 97.94 ResNetDDoS-2: 72.40, 84.41, 19.80, 30.13 ResNetDDoS-3: 58.77, 82.28, 11.53, 19.36 ResNetDDoS-4: 65.81, 75.50, 14.29, 20.25
4	Approach based on the attack-defense tree to assess the relevant countermeasures for protecting IoT infrastructure	IoT network attacks	Quantitative metrics of existing attacks were collected, an Attack-Defense Tree (ADT) was constructed as a logical formula by combining attacks and countermeasures, a countermeasure called “defense configuration” with the highest impact on attacks was provided.	Only a Limited number of attacks have been analyzed and there is a need to introduce more quality metrics like energy.	Attacks were characterized by the following metrics: lower time bound, upper time bound, cost to perform the

			Finally a approach for the automatic identification of impactful countermeasures that can increase the cost of attacks and decrease their probability of success was proposed.		attack, env i.e probability of success.
5	Propose a framework that will strengthen the IoT devices from becoming attack targets and attack source	DoS, Scanning attacks, Botnet activities, attacks from trusted and non-trusted ip sources	Proposed an IoT-Sphere framework that enhances IoT device security by creating a restricted communication sphere of trusted IP addresses. It prevents unauthorized access and attacks while monitoring permitted communication for anomalies using advanced detection engines.	framework's effectiveness in different types of IoT environments or with different types of IoT devices is not discussed, framework's scalability and efficiency in larger, more complex IoT networks is not addressed.	
6	Overview of Security challenges at the application layer and its countermeasures	Sybil attacks, rolling code attacks, brute force attacks, and Buffer overflow attacks , Side channel attacks, spoofing attacks, routing attacks.	Discussed the security in IoT infrastructure at different levels: Information level, functional level and access level.	Only a single countermeasure discussed for each attack	
7	To assess cybersecurity risks of the dynamic device-to-device networks of a smart city.	Major security threats in IoT/IIoT, VANET, and WSN infrastructures	Synthetic datasets are created using the NS-3 simulator, simulating various smart city systems and network attacks. Special coefficients used for dynamic network analysis, and a vector with 38 parameters is formed for modeling. Thresholds for unacceptable risks are independently set for which the neural network achieves a maximum classification accuracy of 97%.	Limited scope	97% accuracy in neural network
8	To examine the security and privacy challenges that arise in the context of Smart Cities	Attacks on smart energy meters, security devices, smart appliances and IoT devices.	Gives insights into the evolution of smart cities and interconnected systems, highlighting key security and privacy challenges. It emphasizes the necessity for privacy protection mechanisms	Very few attacks considered	

			and proposes a model for representing interactions within smart cities. The study also addresses the impact on transportation systems and underscores the need to address security and privacy concerns for future development		
9	This paper examines IoT attacks and provides protective solutions to overcome malicious attacks in IoT and Cloud.	DOS and DDOS SCA(side-channel attacks) Network attacks Server attack	Authentication and authorization initially using various hash function algorithms and encryption of data using cryptographic algorithms. suggests the adoption of a centralized management system like a gateway to monitor and manage low power devices.	Suggest focusing on Ultra-lightweight encryption mechanism, unique default credentials and multifactor authentication to enhance security	
10	Implementing and analyzing the challenges of Incorporating next-generation Lightweight cryptography for smart IoT Devices:	General attacks	Proposes the adoption of Lightweight Cryptography (LWC) as a solution for providing robust security in IoT applications, particularly addressing the limitations posed by low-power processors and memory modules. It discusses the current status of LWC, its compatibility with technologies like LoRaWAN, and highlights challenges through an evaluation of existing academic research and practical studies	Need for more application-oriented and feasible solution in order to optimize security assurance and privay protection.	
11	To propose a hierarchical security framework for defending against sophisticated attacks on Wireless Sensor Networks (WSNs) in smart cities	Dynamic ongoing attacks, Unknown attacks	A hierarchical security framework for enhancing wireless sensor network (WSN) security in smart cities, integrating usage control and chance discovery technologies for advanced persistent threat detection was proposed. It employs dynamic adaptive chance discovery mechanisms alongside software-defined networking and network function virtualization for efficient attack mitigation, validated through experimentation and simulations.	Lack of real world testing, assumption that WSNs are connected through Wi-Fi and limited attack type considered.	Detection Rate (DR) = x/n

4 DDoS (Distributed Denial-of-Service) Attack

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic [48]. In a DDoS attack, the attacker typically uses a network of compromised computers, known as botnets, to send a large volume of requests to the target simultaneously. This flood of traffic consumes the target's bandwidth, processing power, or other resources, rendering the target inaccessible to legitimate users. These attacks can originate from many different sources, making it challenging to mitigate them by simply attempting to block a single source.

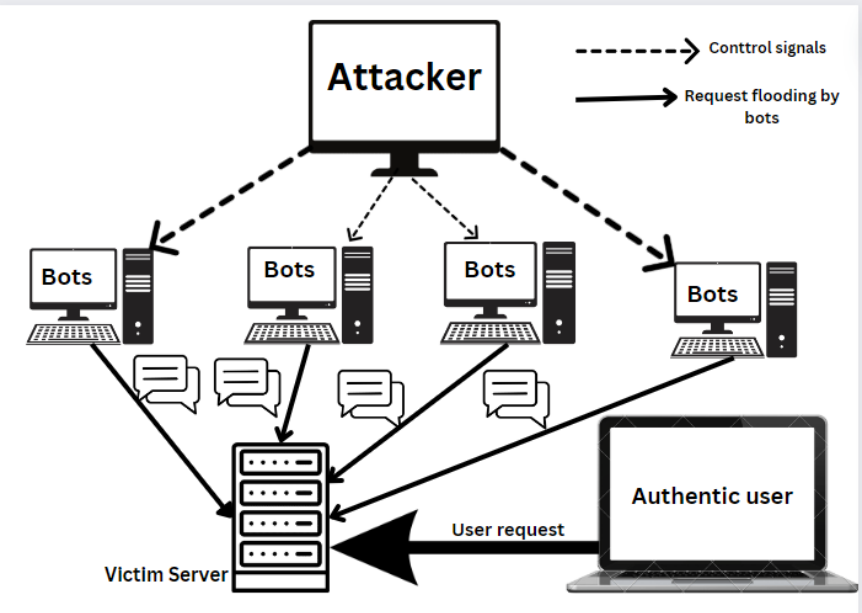

Fig 3: DDoS Attack

DDoS attacks have demonstrated significant and destructive consequences on smart cities, posing a considerable threat to their digital infrastructure and essential services. Consider the following cases:

The largest DDoS attack to date occurred in October 2023, reaching over 398 million requests per second, which was eight times bigger than its predecessor that reached over 46 million rps in 2022 [49].

In Februaury 2023, Web infrastructure company Cloudflare disclosed that it thwarted a record-breaking distributed denial-of-service (DDoS) attack that peaked at over 71 million requests per second (RPS). It was the largest HTTP DDoS attack reported to date, more than 35% higher than the previous 46 million RPS DDoS attack that Google Cloud mitigated in June 2022 [50]

The DDoS attacks on Sweden rose more than fourfold (466%) after the country got accepted into the NATO alliance, [51].

In August 2022, the Finnish parliament's website experienced a DDoS attack while the parliament was in session, causing the government websites to slow down and crash. The attack was coordinated by Russian state-sponsored hackers to disrupt the Finnish government’s websites in retaliation for the application to join NATO.[52]

A DDoS attack targeted numerous Estonian government websites, including those of the president, Ministry of Foreign Affairs, Police and Border Guard, identification card portal, and state services digital portal in the year 2022. Estonia's criticism of the Russian war on Ukraine likely made it a target for Russian hackers [53].

In July 2022, Lithuanian energy company Ignitis Group was hit by the biggest cyber attack in a decade. The pro-Russia group Killnet launched a persistent DDoS attack disrupting the access to the website, targeting Lithuania for its support of Ukraine in its conflict with Russia [54].

Hence, DDoS attacks remain a major cybersecurity threat and a powerful weapon in politically-driven attacks due to their increasing scale, targeted nature against countries and organizations expressing political views, and strategic intent to disrupt critical infrastructure and services.

5 Proposed Work

We suggest a solution that combines a permissioned blockchain network involving participants, lightweight agents for detecting anomalies and sharing evidence, and a reputation-scoring system based on verified evidence on the blockchain. This approach offers an effective method to mitigate and defend against DDoS attacks.

- Leveraging Blockchain: We propose establishing a permissioned blockchain network where participants (such as websites, ISPs, security firms) can join. Unlike public blockchains like Bitcoin,here, the system uses a permissioned blockchain where participants are pre-approved. This improves scalability and reduces the risk of malicious actors joining the network . Each participant will have a reputation score based on their contribution to DDoS mitigation efforts.

- Traffic Analysis: Participants set up lightweight agents(softwere) to keep an eye on network traffic, looking out for any unusual patterns. These agents can use existing methods like analyzing flow rates or setting up honeypots to detect suspicious activity. Instead of putting too much strain on individual systems, these agents spread out the workload. This way, we can handle more traffic without overwhelming our detection methods. Hence proving to be a better method than the traditional one.

  Furthermore, we can leverage quantum technology. Quantum computing presents a compelling opportunity to improve the efficiency of detecting DDoS attacks. Quantum computers parallel processing capabilities enable them to analyze vast amounts of real-time network traffic data, potentially uncovering intricate DDoS attack patterns that classical computers struggle to identify. Quantum algorithms are also adept at recognizing hidden patterns, revealing coordinated attacks across networks or anomalies within encrypted traffic, thereby boosting our detection efficiency.

- Hashed Evidence Sharing: By sharing only hashed data snippets, we can protect privacy while still having enough information to validate the details. It is like sharing only bits and pieces of data that are like coded puzzles just enough to verify what's happening without revealing the whole picture. This is a novel approach to balance information sharing and privacy concerns in a blockchain-based DDoS defense system.

- Reputation Scoring: When an anomaly is detected, the agent(a lightweight software program deployed on various devices throughout the network) submits evidence, that is, hashed data snippets to preserve privacy to the blockchain. This triggers a consensus mechanism where other participants validate the evidence. If validated, the source IP or network associated with the attack receives a negative reputation score on the blockchain. Validated evidence strengthens the reputation system. This discourages false accusations and ensures a fair scoring mechanism. Each participant's contribution to DDoS mitigation efforts is reflected in their score. This incentivizes cooperation and discourages malicious behavior. Similar reputation scores exist, but not necessarily on a blockchain for DDoS defense.

- Mitigation Strategy: Websites and ISPs can access the reputation scores on the blockchain. When a request arrives from a source with a low reputation score, additional challenges (CAPTCHAs, puzzles) can be presented before fulfilling the request. Repeat offenders with very low scores can be temporarily blocked.

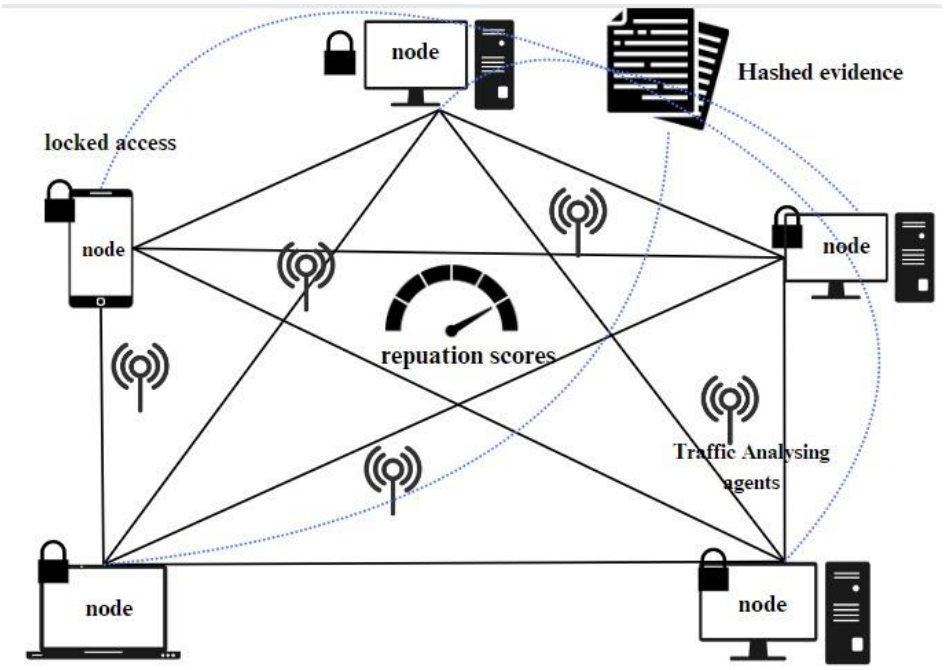

Fig 4: Permissioned blockchain with traffic analysis, hashed evidence and reputation scoring

This reputation-based DDoS defense system combines blockchain's transparency and trustworthiness with distributed traffic analysis for robust detection. Leveraging lightweight agents enables scalable, distributed monitoring, while reputation scoring incentivizes active participation and collaboration among stakeholders, enhancing coordinated defense against DDoS attacks.

6 Implementation Method

A permissioned blockchain network can be developed using platforms like Hyperledger Fabric or Quorum. Smart contracts should be designed and implemented to handle participant registration, evidence submission and validation, and reputation score calculation and storage. Byzantine Fault Tolerance can be employed as the consensus mechanism for validating evidence. Lightweight software agents should be created for network participants, for anomaly detection and implementing hashing algorithms. Secure communication protocols must be established for agents to interact with the blockchain network and reputation scores need to be updated accordingly. A user interface should be designed for participants to access their reputation scores and an API can be developed for websites and ISPs to access reputation scores from the blockchain, integrating them with existing mitigation strategies such as CAPTCHAs and blocking. Other access control mechanisms may also be added,given that the add to the security of proposed mechanism.

7 Discussions And Challenges

An assessment was made on recent cyber attacks in smart cities and a literature survey of major attacks as well as their existing solutions was made. From this, specifically, DDoS attack was chosen and its mitigating strategies were explored and studied.

It was found that the existing solutions dealing with cyber attacks, specifically Distributed Denial of Service (DDoS) attacks are not sufficient and fall short in certain ways.These attacks are quite easy to attempt and the frequency of these attacks have also remained high throughout the years.Thus , the probablility of encountering a novel attack

implementation approach remains high. Relying solely on predetermined rules to counter known attacks is insufficient, as novel attack strategies can still penetrate defenses. Scalability remains a concern, as solutions may not perform adequately in real-world settings under large-scale attacks. Outdated data further complicates mitigation efforts, hindering adaptability to evolving threats.In addition to this , most solutions can be applied only to a particular scenario and are implemented only taregetting that.This demands that the DDoS attacks be analysed periodically in order to provide better and consistent solutions for the future.

Blockchain technology has portrayed immense potential due to a distributed ledger and a decentralized approach making it highly secure but it still not a complete solution in itself at the present .It needs to be explored further with relation to other technical domains to provide a reliable robust solution.

8 Future Work

We suggest exploring the combination of blockchain with emerging technologies like fog and edge computing to enhance security defenses. Prioritizing classical machine learning techniques for practical anomaly detection could be an optimal solution in the near term.Thus , improvement in currently established blockchain and ML methods can be explored.Moreover,our proposed system combining the blockchain reputation scoring with distributed traffic analysis and hash evidence can be explored further by using real time simulations. By refining the core functionalities of the blockchain system with efficient classical algorithms, there's potential for a scalable DDoS defense solution. Concurrently, research on integrating quantum computers for advanced anomaly detection can continue alongside the development of the mitigation system's foundational aspects.

9 Conclusion

In conclusion, the evolving landscape of data security threats in smart cities demands heightened vigilance and proactive measures to safeguard against emerging challenges.

This paper has provided an in-depth examination of the current state of data security issues within smart cities, highlighting the shortcomings of existing approaches and the need for robust countermeasures.

Our proposed solution integrates a permissioned blockchain network with lightweight agents and a reputation-scoring system to effectively counter DDoS attacks in smart cities. This multifaceted approach enhances network security, promotes collaboration among participants, leverages quantum computing for advanced threat detection, and ensures privacy protection while detecting and mitigating cyber threats. By integrating advanced technologies and fostering cooperation, we aim to strengthen data security measures and safeguard sensitive information in smart city environments.

The rise of cyber attacks mandates a fundamental rethinking of our approach to data security, as vulnerabilities in classical computing systems may become increasingly susceptible to exploitation with increasing technological advancements that the future promises. As such, smart cities must be adequately prepared to confront the challenges that lie ahead and ensure the protection of sensitive information in an evolving digital environment. By proactively implementing robust security measures, smart cities can effectively mitigate the dangers posed by data security and stay ahead of potential risks.

9 References

[1] Andrade, R., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020b). A comprehensive study of the IoT cybersecurity in smart Cities. IEEE Access, 8, 228922–228941. https://doi.org/10.1109/access.2020.3046442

[2] Alzyoud, F. Y., Wa'elJum'ah Al_Zyadat, F. H., & Shrouf, F. (2018). A proposed hybrid approach combined QoS with a CR system in a smart city. Eurasian Journal of Analytical Chemistry, 13(6), 178-185

[3] Kalinin, M. O., Krundyshev, V., & Zegzhda, P. D. (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4), 78. https://doi.org/10.3390/machines9040078

[4] Petrolo, R., Loscrí, V., & Mitton, N. (2015b). Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. Transactions on Emerging Telecommunications Technologies, 28(1). https://doi.org/10.1002/ett.2931

[5] Aguilera, U., Peña, O., Belmonte, Ó., & López-De-Ipiña, D. (2017). Citizen-centric data services for smarter cities. *Future Generation Computer Systems*, *76*, 234–247. https://doi.org/10.1016/j.future.2016.10.031

[6] Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. Cities, 38, 25–36. https://doi.org/10.1016/j.cities.2013.12.010

[7] M. Naphade, G. Banavar, C. Harrison, J. Paraszczak, and R. Morris.(2011). Smarter cities and their innovation challenges, Computer,*44*(6), 32–39.

[8] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, ´and D. Barthel. (2011).Security and privacy in your smart city, in Proceedings of the Barcelona Smart Cities Congress.

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

[10] HT News Desk. (2023, October 31). Aadhaar details of 81.5 cr people leaked in India's 'biggest' data breach. *Hindustan Times*. https://www.hindustantimes.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html

[11] C. Ma.(2021),"Smart city and cyber-security; technologies used, leading challenges and future recommendations," Energy Reports, vol. 7, doi: https://doi.org/10.1016/j.egyr.2021.08.124.

[12] N. Moustafa, B. Turnbull, and K.-K.-R. Choo.(2019), ''An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things,'' IEEE Internet Things J., vol. 6(3), 4815–4830,

[13] L. Metongnon and R. Sadre. (2018), ''Beyond telnet: Prevalence of IoT protocols in telescope and honeypot measurements,'' in Proc. Workshop Traffic Meas. Cybersecurity, New York, NY, USA: Association Computing Machinery, 21–26, doi: 10.1145/3229598.3229604.

[14] Ng, A. (2019, November 21). Amazon tells senators it isn't to blame for Capital One breach. CNET. https://www.cnet.com/news/politics/amazon-tells-senators-it-isnt-to-blame-for-capital-one-breach/

[15] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3). https://doi.org/10.1002/ett.3677

[16] M. Naphade, G. Banavar, C. Harrison, J. Paraszczak, and R. Morris.(2011), "Smarter cities and their innovation challenges," Computer,44(6),32–39.

[17] CrowdStrike. (2024, February 21). What is Cyber Espionage? – CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

[18] CrowdStrike. (2024b, February 21). What is Cyber Espionage? – CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

[19] Gcore. (2023, August 29). What is a denial of service attack? | GCore. https://gcore.com/learning/what-is-denial-of-service-attack/

[20] Anwar, H. (2024, February 3). Former CIA software developer sentenced to 40 years in prison for confidential data breach to WikiLeaks. Digital Information World. https://www.digitalinformationworld.com/2024/02/former-cia-software-developer-sentenced.html

[21] Ikeda, S. (2023, March 10). Ransomware attack on Barcelona Hospital threatened urgent care cases, locked up patient records. CPO Magazine. https://www.cpomagazine.com/cyber-security/ransomware-attack-on-barcelona-hospital-threatened-urgent-care-cases-locked-up-patient-records/

[22] Greig, J. (2021, October 22). 450 million cyberattacks attempted on Japan Olympics infrastructure: NTT. ZDNET. https://www.zdnet.com/article/nearly-450-million-cyberattacks-attempted-on-japan-olympics-infrastructure-ntt/

[23] Sea, E. (2023, June 23). Singapore phishing targets increased to 8,500 and ransomware attacks stood at 132 in 2022: CSA. ETCIO.com. https://ciosea.economictimes.indiatimes.com/news/security/singapore-phishing-targets-increased-to-8500-and-ransomware-attacks-stood-at-132-in-2022-csa/101204794

[24] Petkauskas, V. (2022, November 25). FC Barcelona's official website exploited for fraud. Cybernews. https://cybernews.com/news/fc-barcelona-official-website-fraud/

[25] Sun, D. (2023, June 6). Hacker steals luxury retailer Cortina Watch's data, including customer details. The Straits Times.https://www.straitstimes.com/singapore/hacker-steals-data-of-luxury-retailer-cortina-watch-including-customer-details

[26] Paganini, P. (2023, December 12). Dubai's largest taxi app exposes 220K+ users. Security Affairs. https://securityaffairs.com/155695/security/dubai-taxi-company-data-leak.html

[27] Holden, M. (2023, December 13). UK defence ministry fined for Afghan data breach during Taliban takeover. https://www.reuters.com/world/uk/uk-defence-ministry-fined-afghan-data-breach-during-taliban-takeover-2023-12-13/

[28] Hope, A. (2023, September 7). Staggering data breach exposed 47,000 London Met police officers and staff. CPO Magazine. https://www.cpomagazine.com/cyber-security/staggering-data-breach-exposed-47000-london-met-police-officers-and-staff/

[29] A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures. (2018, September 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8656694

[30] Aggressive jamming attack in IoT networks. (2022, December 6). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9998231

[31] A Two-Fold Machine learning approach to prevent and detect IoT botnet attacks. (2021). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9627657

[32] Exploration of impactful countermeasures on IoT attacks. (2020, June 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9134200

[33] IoT-Sphere: A Framework to Secure IoT Devices from Becoming Attack Target and Attack Source. (2020, December 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9343016

[34] Classification of various types of attacks in IoT environment. (2020, September 25). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9242592

[35] Kalinin, M. O., Krundyshev, V., & Zegzhda, P. D. (2021b). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), 78. https://doi.org/10.3390/machines9040078

[36] Elmaghraby, A., & Losavio, M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research, 5(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

[37] Cryptography Attacks: 6 Types & Prevention. (2022, August 26). Packetlabs. https://www.packetlabs.net/posts/cryptography-attacks/

[38] Next Generation Lightweight Cryptography for smart IoT devices: : Implementation, challenges and applications. (2019, April 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8767250

[39] Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci.(2002), E. Wireless Sensor Networks: A Survey. Comput. Netw. 38, 399–422.

[40] M, U., & Padmavathi, G. (2013). A survey on various cyber-attacks and their classification. International Journal of Network Security, 15(5), 390–395. https://doi.org/10.6633/ijns.201309.15(5).09

[41] M, U., & Padmavathi, G. (2013). A survey on various cyber-attacks and their classification. International Journal of Network Security, 15(5), 395–396. https://doi.org/10.6633/ijns.201309.15(5).09

[42] A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. (2016). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/7383218

[43] Khan, Zohaib & Danish, Syed & Qureshi, Hassaan & Lestas, Marios. (2019). Protecting IoTs from Mirai Botnet Attacks Using Blockchains. 1-6. 10.1109/CAMAD.2019.8858484.

[44] Ibrahim, Rahmeh Fawaz, Qasem Abu Al-Haija, and Ashraf Ahmad. 2022. "DDoS Attack Prevention for Internet of Thing Devices Using

Ethereum Blockchain Technology" *Sensors* 22, no. 18: 6806. https://doi.org/10.3390/s22186806

[45] C. Liu, J. Yang, R. Chen, Y. Zhang and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," 2011 Seventh International Conference on Natural Computation, Shanghai, China, 2011, pp. 212-216, doi: 10.1109/ICNC.2011.6022060.

[46] *Research on immunity-based intrusion detection technology for the Internet of Things*. (2011, July 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/6022060

[47] Cheng, J., Wu, Y., Yuepeng, E., You, J., Li, T., Li, H., & Ge, J. (2021b). MATEC: A lightweight neural network for online encrypted traffic classification.*Computer Networks*,*199*,108472. https://doi.org/10.1016/j.comnet.2021.108472

[48] *What is a distributed denial-of-service (DDoS) attack? | Cloudflare*. (n.d.). https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[49] Mulyandari, R. (2024, April 19). *What developers can learn from the largest DDoS attack in history*. Developer Tech News. https://www.developer-tech.com/news/2024/apr/19/what-developers-can-learn-from-largest-ddos-attack-in-history/

[50] The Hacker News. (n.d.). *Massive HTTP DDoS attack hits record high of 71 million Requests/Second*. https://thehackernews.com/2023/02/massive-http-ddos-attack-hits-record.html

[51] FadilpaŠI, S. (2024, April 17). DDoS attacks saw a huge surge in the first part of 2024, with one particular country badly hit. *TechRadar*. https://www.techradar.com/pro/security/ddos-attacks-saw-a-huge-surge-in-the-first-part-of-2024-with-one-particular-country-badly-hit

[52] Ciso, E. (2022, August 10). Finnish parliament website targeted in cyber attack. *ETCISO.in*. https://ciso.economictimes.indiatimes.com/news/finnish-parliament-website-targeted-in-cyber-attack/93470177#:~:text=Helsinki%2C%20Aug%209%2C%202022%20%2D,parliament%20said%20in%20a%20statement.

[53] *Recent cyber attacks in 2022 | Fortinet*. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks

[54] Bns. (2022, July 11). Lithuania's state-owned energy group hit by "biggest cyber attack in a decade." *lrt.lt*. https://www.lrt.lt/en/news-in-english/19/1736266/lithuania-s-state-owned-energy-group-hit-by-biggest-cyber-attack-in-a-decade