Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.054007 Published Online: 13 September 2024

ARTICLE

Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach

Mehdi Houichi[1,*], Faouzi Jaidi[1,2] and Adel Bouhoula[3]

[1]University of Carthage, Higher School of Communication of Tunis (Sup'Com) Innov'Com Lab\Digital Security Research Lab, Tunis, 2083, Tunisia

[2]National School of Engineers of Carthage, University of Carthage, Tunis, 2035, Tunisia

[3]Department of Next-Generation Computing, College of Graduate Studies, Arabian Gulf University, Manama, 26671, Kingdom of Bahrain

*Corresponding Author: Mehdi Houichi. Email: mehdi.houichi@supcom.tn

Received: 16 May 2024 Accepted: 15 August 2024

ABSTRACT

The expansion of smart cities, facilitated by digital communications, has resulted in an enhancement of the quality of life and satisfaction among residents. The Internet of Things (IoT) continually generates vast amounts of data, which is subsequently analyzed to offer services to residents. The growth and development of IoT have given rise to a new paradigm. A smart city possesses the ability to consistently monitor and utilize the physical environment, providing intelligent services such as energy, transportation, healthcare, and entertainment for both residents and visitors. Research on the security and privacy of smart cities is increasingly prevalent. These studies highlight the cybersecurity risks and the challenges faced by smart city infrastructure in handling and managing personal data. To effectively uphold individuals' security and privacy, developers of smart cities must earn the trust of the public. In this article, we delve into the realms of privacy and security within smart city applications. Our comprehensive study commences by introducing architecture and various applications tailored to smart cities. Then, concerns surrounding security and privacy within these applications are thoroughly explored subsequently. Following that, we delve into several research endeavors dedicated to addressing security and privacy issues within smart city applications. Finally, we emphasize our methodology and present a case study illustrating privacy and security in smart city contexts. Our proposal consists of defining an Artificial Intelligence (AI) based framework that allows: Thoroughly documenting penetration attempts and cyberattacks; promptly detecting any deviations from security standards; monitoring malicious behaviors and accurately tracing their sources; and establishing strong controls to effectively repel and prevent such threats. Experimental results using the Edge-IIoTset (Edge Industrial Internet of Things Security Evaluation Test) dataset demonstrated good accuracy. They were compared to related state-of-the-art works, which highlight the relevance of our proposal.

KEYWORDS

Smart cities; digital communications; cybersecurity; privacy; intrusion detection

1 Introduction

Smart cities are commonly defined by their adoption of technology-driven solutions designed to improve citizens' quality of life, encourage increased interaction between the public and government, and support sustainable development initiatives [1]. Smart cities integrate elements of social, environmental, and economic advancement through decentralized approaches, enabling more effective management of critical resources, urban dynamics, and real-time operations. Strategically planned, these cities feature an information and communication technology (ICT) infrastructure, leveraging Internet of Things (IoT) sensor technologies to promote social and urban connectivity, thereby enhancing public participation and governmental efficiency [2]. Numerous cities worldwide have embraced the concept of smart cities, either by enhancing their existing infrastructure to attain this status or actively seeking ways to adapt their current resources and networks [3]. These cities are New York, Stockholm, Dubai, London, Amsterdam, Reykjavik, Paris, Tokyo, Busan.

In a bid to promote economic expansion through technology-driven solutions for citizen engagement, the Government of India (GoI) has announced intentions to develop 100 smart cities nationwide [4]. In China, a government-led, top-down approach has resulted in a notable expansion of smart city initiatives, considered deliberate policy decisions aimed at potentially restructuring economic frameworks, advancing economic progress, retraining and enhancing workforce competitiveness, and augmenting governmental efficiency and efficacy [5]. Various components within smart cities can interface and interact with the network infrastructure, utilizing modern technologies like sensors, mobile cloud computing, networks, electronic devices, and machine learning technologies [6]. Processing and managing data are one of the major difficulties in creating smart cities. This pertains to existing data within city systems and the integration of data with emerging platforms and sensors within the smart city environment, impacting security and privacy [7]. The significance of tackling information security, data privacy, and cyber threats early in the design and development phases of smart cities is highlighted by the potential risks, including unauthorized data access leading to adverse consequences [8]. As smart city applications exhibit vulnerabilities, individuals may encounter various security and privacy concerns as cities evolve [9]. For instance, nefarious actors might tamper with data to skew sensing outcomes, affecting services, decisions, and governance within smart city environments. Moreover, these perpetrators may launch denial-of-service attacks to disrupt sensing, transmission, and control, thereby compromising the quality of intelligent services in smart cities. Additionally, the extensive video surveillance systems in smart cities capture a vast amount of images and videos, which could be used to infer residents' movements and pose privacy risks [10]. While existing techniques and practices (such as encryption, authentication, and anonymity) may directly address these issues, there are still numerous avenues for sophisticated attackers to exploit privacy, such as side channel attacks and cold boot attacks. Without adequate security and privacy measures, the adoption of smart cities by the public may be hindered [11].

The following sections of this paper are organized as: Section 2 furnishes background information pertaining to smart cities, encompassing their benefits and architecture. Section 3 delves into intrusion detection systems. Following this, Section 4 examines the threat model within a smart city context and outlines associated research challenges. Technical insights into the architecture of our system are expounded upon in Section 5. In Section 6, we will evaluate and analyze the performance of the proposed system. Additionally, this section will scrutinize the outcomes and outline future plans for this study. It is dedicated to the conclusions and perspectives derived from this research endeavor in the end.

2 State of the Art of Smart City

2.1 Smart City Applications

The main objectives of smart cities include fostering economic growth and improving residents' quality of life [12]. These two objectives can be accomplished by improving efficiency, sustainability, enabling citizen participation, and enhancing decision-making through enhanced information accessibility. Several proposals or implementations of smart city applications have been put forth to attain this objective [13]. To achieve these objectives, a variety of smart city services are often integrated and interconnected, as depicted in Fig. 1. Intelligent services provided by smart cities, such as smart mobility, smart utilities, smart buildings, smart environment, smart public services, smart governance, smart economy, smart healthcare, and smart citizens, play a crucial role in transforming urban environments. These services leverage advanced technologies to optimize urban operations, enhance resource management, and improve the overall well-being of residents.

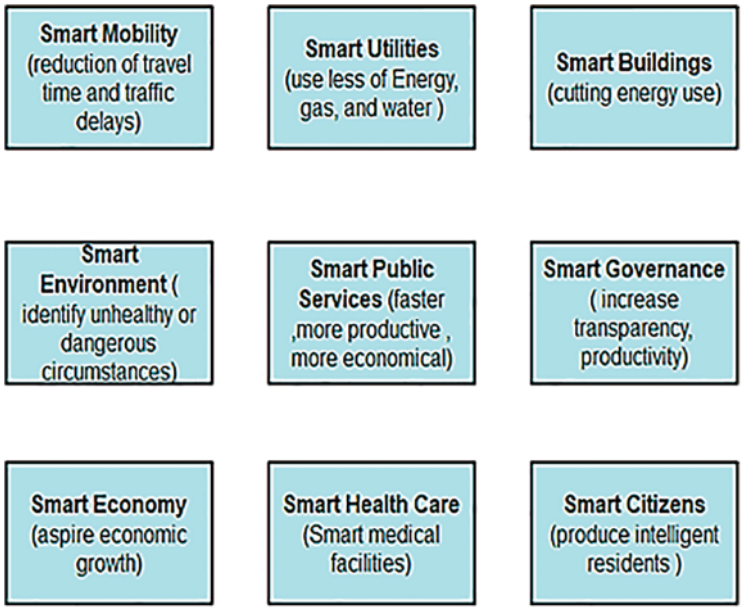

Figure 1: Smart city applications

Smart Mobility: Moving on to smart mobility, a key feature frequently linked with smart cities is a sophisticated transportation system [14]. This system aims to improve traffic safety and efficiency, decrease commuting time, and elevate residents' overall quality of life. It encompasses both private and public transportation, with applications designed to equip intelligent vehicles with advanced sensor technology and communication networks. These features enable enhanced driver assistance and potentially autonomous driving capabilities. Furthermore, efforts to reduce travel times and CO_2 emissions, as well as improve traffic flow, include the implementation of intelligent, adaptive traffic lights [15]. Geolocation services, facilitating users in finding the nearest gas station, electric vehicle charging station, or available parking spaces, play a pivotal role in mitigating delays and enhancing traffic flow within urban areas [16]. Additionally, on a broader scale, strategies such as minimizing traffic congestion during peak hours and public events, optimizing bus routes, and promoting shared bike programs alongside cycling lane networks all contribute to alleviating traffic congestion and reducing air pollution [17].

Smart Utilities: Energy, gas, and water consumption are examples of resources that smart utilities aim to minimize, contributing to both economic expansion and sustainability [18]. Smart grids, decentralized energy storage and virtual power plants are widely recognized examples of smart utility applications. These systems may also involve electric vehicles or decentralized electricity generation, often facilitated by the deployment of smart metering devices. Further instances of smart utilities comprise activities like monitoring water resources, regulating water pressure, and flexibly incorporating both conventional and renewable energy sources in response to present and anticipated electricity requirements [19].

Smart Buildings: Smart buildings aim to increase the energy and efficiency of residential and commercial spaces [20]. For example, they can adjust lighting and temperature based on people's activities and use smart devices to improve daily tasks. Additionally, smart buildings can closely monitor structural integrity. The concept of home automation, often referred to as 'smart home', has become popular. Smart home increases energy efficiency and creates comfort by combining a sensor network with an active motor [21].

Smart Environment: The main purpose of a smart environment is to improve urban development and increase people's quality of life and safety. This can be achieved by generating maps of noise and air pollution, among other measures [22]. With such a map, authorities can quickly detect abnormal or dangerous conditions and take appropriate action, such as imposing road restrictions, issuing public warnings, or even evacuating cities entirely. Sensor networks can also detect disasters such as earthquakes, volcanic eruptions, hurricanes, floods and forest fires [23]. Early warning systems play an important role in reducing loss of life and property. Ideally, the system will work with other smart city components, such as smart transportation to manage traffic in hazardous areas or smart actions to cut off electricity in hazardous areas.

Smart Public Services: The objective of smart public services is to ensure the efficient and effective utilization of public resources. These services encompass various applications, including adaptive waste management strategies such as optimizing waste collection routes or deploying smart trash cans equipped with sensors that notify authorities when they reach capacity [24]. Additionally, crisis management and response applications can equip first responders with crucial information and resources, including building layouts. Deploying distributed technologies such as network cameras or audio monitoring systems can further increase the efficiency and effectiveness of public safety services. Another noteworthy example is energy-efficient smart street lighting that adjusts its intensity based on the presence of pedestrians and cyclists, thereby enhancing overall traffic safety [25].

Smart Governance: The objective of smart governance is to enhance transparency, increase local government productivity, and tailor services to meet the needs of citizens [26]. Open data processing increases efficiency and transparency by allowing users to access and reference a variety of data. In addition, e-government services allow citizens to carry out various interactions with the government online, such as planning a wedding or applying for social housing, a residence permit or school admission. Additionally, individuals can actively participate in urban planning and development through mobile applications for reporting, online community forums, and community forums to receive feedback on the development of their city [27].

Smart Economy: The smart economy aims to improve the economy through new business activities such as consultancy services and partnerships between the public and private sectors. Additionally, new business models are founded on efforts to combine data from various sources and expand open data availability. Cities can promote entrepreneurship by providing affordable broadband connectivity, supporting startup office spaces, and fostering entrepreneur networks [28].

Smart Healthcare: Smart healthcare involves the effective and efficient delivery of medical treatment. For instance, smart medical facilities have the capability to integrate patient health records from various sources, thereby enhancing the quality of medical care [29]. Data obtained from wearables and interconnected medical equipment are also valuable assets in smart healthcare initiatives. Residents can access healthcare services through telehealth to minimize waiting and travel times. Additionally, smart medical applications aim to empower patients by giving them control over their health and disease-related information.

Smart Citizens: Smart cities aspire to empower individuals to foster informed residents and cohesive communities [30]. For example, smart education initiatives encompass lifelong learning programs targeting various aspects such as employability, digital inclusion, or specific demographics like autistic children. Providing subsidized internet connectivity in underserved areas can aid residents, while interactive information kiosks serve to connect both locals and visitors to a wide array of services.

Smart City Applications (Environmental Monitoring and Utilization): In this section, I have outlined the various intelligent services that smart cities offer. These services leverage a variety of technologies to monitor and utilize the physical environment effectively, enabling the delivery of intelligent services. This includes deploying sensor networks to gather real-time data on air quality, noise levels, and other environmental parameters. Internet of Things (IoT) devices, such as smart meters, monitor energy and water consumption, promoting resource efficiency. Geospatial technologies and satellite imagery provide detailed insights into land use, environmental changes, and disaster impacts. Advanced data analytics and artificial intelligence process this data for predictive modeling and decision support. Citizen engagement platforms further enhance transparency and resident participation in urban environmental management. Together, these tools enable smart cities to optimize operations, enhance sustainability, and improve the overall quality of life for their residents.

2.2 Enabling Technologies

The innovation and technology of a smart city derive mainly from the use of supporting technologies rather than the use itself [31]. Through our literature review, we have divided common technologies relevant to the 'smart city' concept into nine different categories: wearable technology, ubiquitous connectivity, smart maps, sensor networks, smart vehicles, autonomous systems, cloud computing and open data, as shown in the Fig. 2.

These technologies themselves have been enabled by earlier technological developments. Embedded systems, for example, have greatly accelerated ubiquitous and pervasive computing. The ability to perform complex operations on portable devices or even household appliances is made possible by smaller, faster microprocessors. The lifespan of mobile devices and outdoor sensors is extended by energy-efficient processors and durable batteries [32]. Even the smallest objects can contain communication capabilities that allow them to be integrated into smart city networks using radio technology, such as passive RFID tags and microstrip antennas. Most smart city projects use a combination of two or more of these core technologies. For example, the capacity to monitor noise and air pollution citywide in real-time, facilitated by pervasive connectivity and participatory sensor networks, contributes to creating a more intelligent environment. The integration of these technologies underpins the foundational framework of smart cities, demonstrating their collective role in enhancing urban efficiency and sustainability.

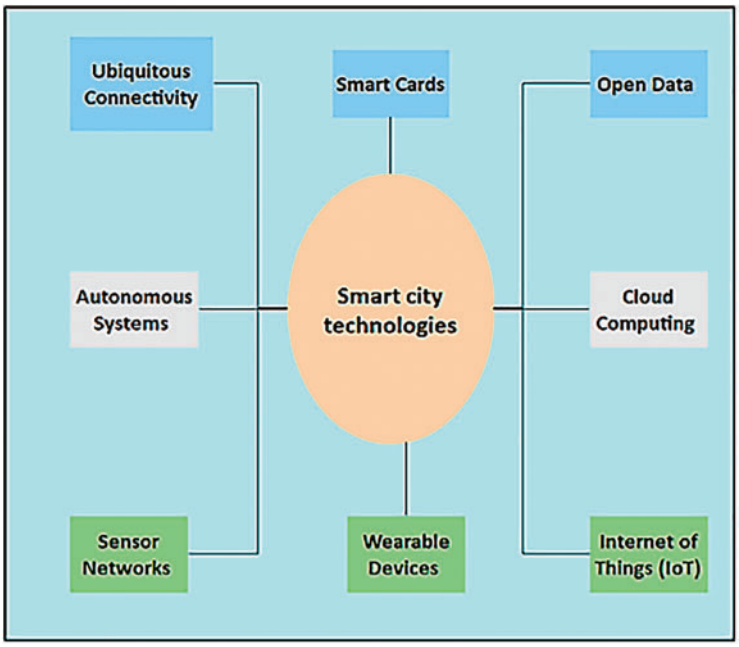

Figure 2: Smart city technologies

Ubiquitous Connectivity: Many services rely on user devices that require internet connectivity, such as smartphones, tablets, smart devices or smart gadgets. In urban settings, the majority of households now have access to broadband internet via landline connections, with the availability of high-speed cellular networks like 4G expanding rapidly. Emerging technologies like 5G and compact cells are poised to fully support the next wave of smart city applications [33]. However, opting for a WiFi connection over cellular offers certain advantages. For instance, transferring large media files may not be feasible due to data volume limits often associated with cellular internet plans. Moreover, some users, like international travelers, may lack cellular internet plans, relying instead on alternative means to access the internet. In such scenarios, initiatives providing free internet access through public WiFi, possibly offered by municipal authorities, businesses, or private user groups, can effectively serve as a substitute for cellular connectivity [34].

Smart Cards: Today's smart cards have evolved to enable cashless transactions, transfer legal information, and even serve as driver's licenses and other travel documents. Although smart cards have been around for a long time, the emergence of wireless smart cards and the integration of smart card readers have brought about many new applications. The ISO/IEC 14443 standard forms the basis of modern smart cards, which combine written memory, microprocessor and short circuit technology [35]. To enable online control of multiple smart card devices, all data must be stored in the smart card database, which can only be accessed by the smart card reader or writer. Additionally, smart card readers can be connected to a backend server to provide advanced security measures and accounting functions [36].

Open Data: It is defined as information that is technically available to the public and legally permissible for use and analysis by outside parties. Through the facilitation of third-party service provision leveraging city data, open data initiatives have the potential to foster innovation and augment government transparency. Cities may opt to utilize open-source portals as a means to divulge data [37].

Sensor Networks: Sensor networks serve as the cornerstone of numerous smart city applications, spanning smart public services, smart environments, smart buildings, and smart mobility. Essentially, they act as data collectors, furnishing the necessary information for well-informed, and potentially automated, decision-making and actions. Illustrative examples include air quality monitoring, fire detection, closed-circuit television (CCTV) systems, and induction loops when integrated with a central traffic control facility. Cities aspire to broaden sensor availability and coverage to encompass every facet of urban areas [38]. Smart city sensor networks have the potential to integrate the sensing capabilities of consumer electronics like smartphones. This phenomenon is often called participatory sensing, crowd sensing, or opportunistic sensing. Furthermore, sensors facilitate location-based services, particularly now that portable GPS, GLONASS, and Galileo receivers are readily available.

Wearable Devices: Wearable devices or body area network data, unlike data produced by sensor networks, almost invariably generate personal data unique to the wearer. These devices monitor various physical activities such as heart rate, blood pressure, and brain activity [39]. Subsequently, these readings can be relayed to medical professionals via communication technology, thus improving healthcare. In addition to applications for whole-body monitoring in hospitals, wearable devices can also be useful in other settings, such as private homes, where vital signs of people with chronic diseases can be monitored. The United States Communications Commission has already published a separate line for these two programs. Entertainment wearable devices such as smartwatches and fitness trackers are also becoming popular [40]. Other examples of wearable devices that can work with smart city technology and applications include smart glasses and interactive, augmented reality systems. The widespread adoption of environmental and health monitoring will be further facilitated by smart nanotextiles equipped with sensing, actuation, and communication capabilities [41].

The Internet of Things (IoT): As defined by [42], the Internet of Things (IoT) represents "a global infrastructure for the information society, facilitating advanced services through the interconnection of (physical and virtual) objects using interoperable information and communication technologies." Essentially, IoT entails enhancing everyday objects with sensors, actuators, and communication devices, frequently integrated with big data services. Unlike sensor networks, the IoT involves adding sensing and communication capabilities to an object's functionality or service it offers rather than being its primary feature. Examples of this include smart refrigerators, smart meters, and smart air conditioning units [43].

Autonomous Systems: In forthcoming urban landscapes, autonomous systems often embodied as robots will play a vital role. For example, the shift from individually owned vehicles to shared autonomous transportation could fundamentally alter commuting patterns. Moreover, autonomous systems can undertake city tasks like waste collection, street cleaning, and even aerial surveillance using drones programmed for autonomous operation [44].

Intelligent Vehicles: Equipped with an array of sensors, communication tools, or autonomous driving capabilities, intelligent vehicles can tap into cellular technology for accessing centralized services such as traffic updates or emergency assistance. They can also communicate with infrastructure elements like traffic signals and dynamic road signs or share information spontaneously. In North America and Europe, ad-hoc communication based on IEEE 802.11p has already been standardized. Additionally, the rise of ride-sharing and driverless taxi services stands to reshape urban mobility [45]. Given that the average car remains parked for 23 h daily, these systems hold substantial potential for reducing vehicular congestion.

Cloud Computing: Cloud computing entails delegating computational tasks to external entities that provide hardware infrastructure, operating system platforms, or entire software applications as

a service. With cloud computing, the upfront capital expenditure for IT hardware is transformed into a recurring cost based on service usage [46]. Cloud services enable rapid and efficient scalability in response to user demand, a crucial aspect in smart cities for ensuring the accessibility of web services to the public or scaling data analysis operations based on information collected throughout the city [47].

Smart cities leverage IoT technology to enhance the quality of life for their residents through improved efficiency and responsiveness of urban services. For example, smart streetlights can adjust their brightness based on the presence of pedestrians or vehicles, thereby saving energy and enhancing safety. IoT-enabled water meters help detect leaks and manage water usage more efficiently, while smart waste bins notify waste collectors when they need to be emptied, optimizing collection routes and reducing waste overflow. Furthermore, intelligent transportation systems utilize real-time data sharing between vehicles and traffic management centers to reduce traffic congestion and improve mobility. This interconnected ecosystem not only improves daily living conditions but also fosters a more sustainable and efficient urban environment.

2.3 Smart City Architecture

The objective of a smart city is to offer intelligent services by leveraging information gathered from the physical realm, transmitted through communication channels, and processed in the digital sphere. This facilitates pervasive sensing and enhances urban governance. As depicted in Fig. 3, it includes processing units, control and operational components, heterogeneous network infrastructure, and sensing components [48].

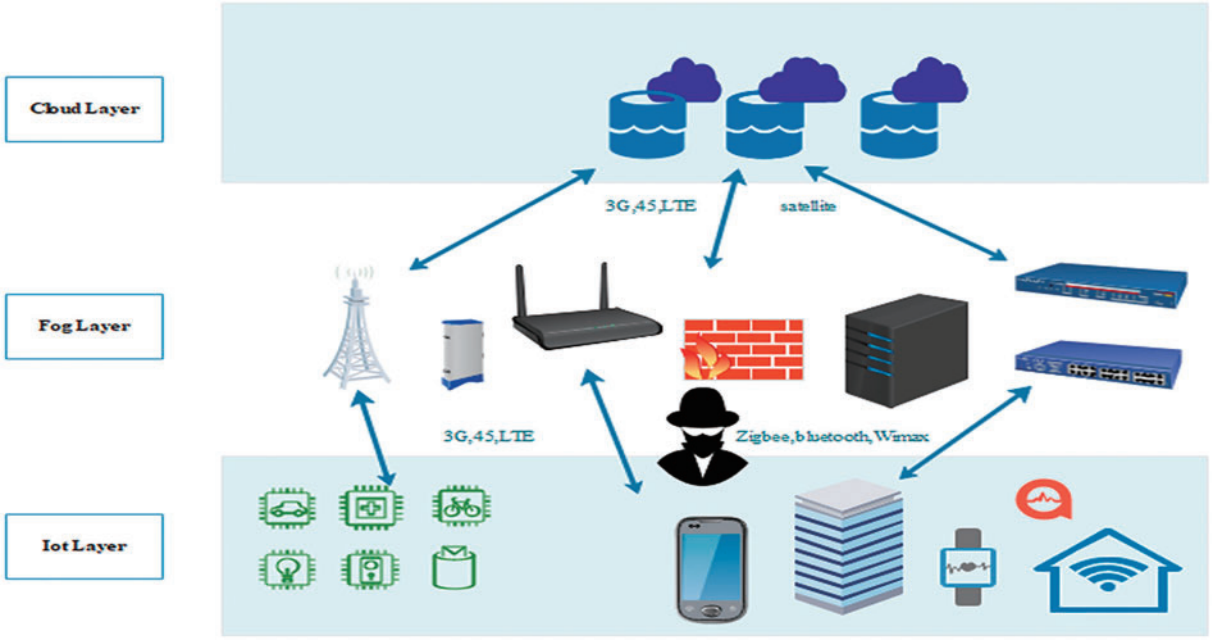

Figure 3: Smart city architecture [49]

Sensing Components: Various devices, including wearables, smart gadgets and industrial sensors like smart meters, smartphones and security cameras, serve as sensing components to gather data from the physical world. Following that, the data is transferred to the processing unit to make decisions,

serving as the vital bridge between the realms of information and physical reality. These sensing devices are either carried by users or deployed by government entities, ministries, and businesses. Considering limitations such as device dimensions, battery longevity, and processing capacity, these sensing devices with restricted resources often undertake preliminary processing or compression of real-time and detailed data before transmitting it to the network [50].

Heterogeneous Networks: The infrastructure of heterogeneous networks is fundamental in enabling the functionality of a smart city, facilitating the coexistence of various applications and sensing devices. This infrastructure allows for diverse methods of collecting sensing data by incorporating cellular networks, sensor networks, wireless local area networks (WLANs), wide area networks (WAN), device-to-device (D2D) communications, millimeter-wave communications, and more. By seamlessly integrating different network types, heterogeneous networks serve as a conduit between the physical and digital worlds in a smart city [51].

Processing Unit: The processing unit employs resilient cloud computing servers, expansive databases, and tailored control systems to evaluate and process the gathered sensing data from the physical environment for decision-making purposes. This unit governs the informational landscape of a smart city, requiring certain privileges and authorizations for authorized entities like government bodies, hospitals, factories, and users to access the gathered information. Additionally, it establishes rules or guidelines for decision-making and management within the smart city [52]. The vast amount of data generated by IoT devices in smart cities is managed and analyzed through advanced data analytics platforms and cloud computing. These platforms enable real-time processing, storage, and analysis of data, ensuring timely and informed decision-making.

Control and Operating Components: In a smart city, control and operational aspects like smartphones empower the city to impact the physical realm through feedback generated by optimization and decisions made by the processing unit [53]. These components refine and adjust the physical environment to improve the city's quality of life. Additionally, they facilitate bidirectional information exchange within the smart city, covering both sensing and control tasks. This extensive flow of information guarantees the monitoring and management of every device or element within the smart city, ensuring its seamless and effective operation [53].

2.4 Characteristics of Smart Cities

Understanding the disparities between the mentioned smart applications and conventional ones is crucial. Additionally, prior to devising any new security or privacy protection strategy, it is essential to thoroughly analyze and incorporate the characteristics unique to smart cities, as depicted in Fig. 4.

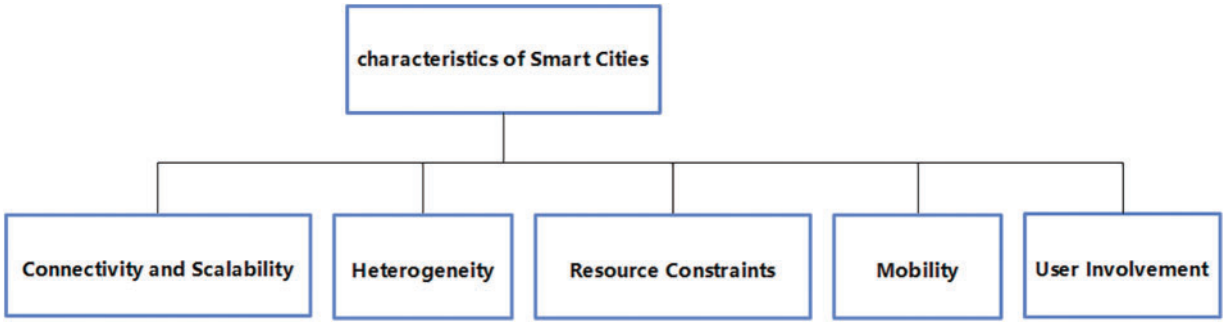

Figure 4: Characteristics of smart cities

Heterogeneity: The defining characteristic of IoT-based systems lies in their considerable heterogeneity, encompassing their autonomous nature, dispersed deployment, and utilization by a multitude of users. This diversity extends to various aspects such as IoT nodes, connectivity technologies, mobility options, hardware capabilities, and platforms [54]. It's noteworthy that each smart city possesses its unique IoT architecture, and there exists no universal definition for a smart city. Consequently, a significant challenge arises from the lack of a standardized security framework and service across different smart city implementations [55].

Resource Constraints: The majority of IoT devices are constrained by limited memory, battery life, computing power, and network interfaces due to their utilization of low-power radio protocols. In general, smart cities utilize embedded devices that are compact, cost-effective, but not as energy-efficient. These devices frequently have limited storage and random-access memory capacities, usually equipped with 8-bit or 16-bit microcontrollers. Wireless networks with IEEE 802.15.4 radio technology also contribute to slow data speeds (ranging from 20–250 kb/s) and small frame sizes (up to 127 octets) [56].

Mobility: Urban mobility plays a pivotal role in the contemporary development of cities, encompassing both intra-city movement and the transportation of goods. Smart city mobility incorporates technologies like citywide wireless communication, real-time traffic monitoring, and adaptive problem-solving. The sophisticated connectivity infrastructure of smart cities facilitates customized transportation solutions to meet changing mobility demands [57].

Connectivity and Scalability: Connectivity serves as the foundational element for any device to join the smart city ecosystem, playing a fundamental role in advancing smart city initiatives. Simultaneously, scalability is a critical consideration in smart city deployments. As smart cities evolve from small-scale implementations to expansive urban landscapes, there's a surge in data and network traffic. Thus, scalable systems and mechanisms are indispensable for the effective operation of smart cities [58].

User Involvement: Beyond technological advancements and infrastructural development, the essence of smart cities lies in benefiting people. Smart city initiatives extend beyond technology to encompass human aspects such as learning, creativity, and education. Community engagement is vital for enhancing the quality and effectiveness of smart applications. Effective security measures, for instance, stem from a deep understanding of users' needs and concerns, highlighting the importance of early user involvement in smart city planning [59].

2.5 Discussion

In summary, smart cities embody a revolutionary strategy for urban progress, harnessing cutting-edge technologies to elevate efficiency, sustainability, and the overall well-being of inhabitants. Smart cities rely on a diverse array of data generated by IoT devices to optimize and enhance urban services. Environmental sensors collect data on air quality, temperature, and humidity, which city officials use to monitor pollution levels and implement measures to improve air quality. Traffic sensors gather information on vehicle counts, speed, and congestion, enabling real-time traffic management and reducing travel time for residents. Smart meters for energy and water usage provide detailed consumption patterns, helping utilities optimize distribution and encourage conservation efforts. Additionally, IoT-enabled waste bins generate data on fill levels, ensuring timely waste collection and preventing overflows. This extensive data collection and analysis enable smart cities to provide efficient, responsive, and sustainable services, significantly improving the quality of life for their

residents. Data analysis in smart city environments offers key benefits such as improved decision-making, efficient resource management, enhanced public services, and increased sustainability. However, it also presents challenges including data privacy concerns, the need for robust cybersecurity measures, handling the vast volume of data, and ensuring interoperability among diverse systems. Characterized by ubiquitous connectivity, data-driven insights, integration of emerging technologies, and a citizen-centric approach, smart cities embody a vision of interconnected urban ecosystems where digital innovation drives progress. However, alongside these opportunities come significant security challenges. Cybersecurity risks, data privacy concerns, infrastructure resilience, and the evolving threat landscape pose formidable obstacles to the realization of smart city objectives. To address these challenges, innovative security methods and solutions are imperative. A comprehensive approach, including proactive threat detection, strong encryption techniques, resilient infrastructure planning, and collaborative initiatives between public and private sectors, is essential to strengthen the digital resilience of smart cities and maintain their effectiveness amidst the challenges of urban environments.

3 Security and Cyber-Security Challenges in Smart Cities

Despite the impressive advancements in smart city technologies, virtually all smart applications remain vulnerable to contemporary cyber threats, including various types of attacks such as background knowledge attacks, collusion attacks, Sybil attacks, eavesdropping attacks, spam attacks, likability attacks, inside curious attacks, outside forgery attacks, and identity attacks [60]. In recent years, numerous instances across various application domains have underscored significant vulnerabilities. For instance, within smart grid systems, the infrastructure of smart meters may inadvertently expose individuals' daily routines and work patterns.

Moreover, both device manufacturers and service providers could potentially access private information within the contexts of smart homes and healthcare. Additionally, users' positions and mobility behaviors can be inferred from the extensive trajectory data collected by smart mobility applications. These concerns underscore the ongoing challenges posed by the rapidly evolving landscape of smart application development, as depicted in Fig. 5.

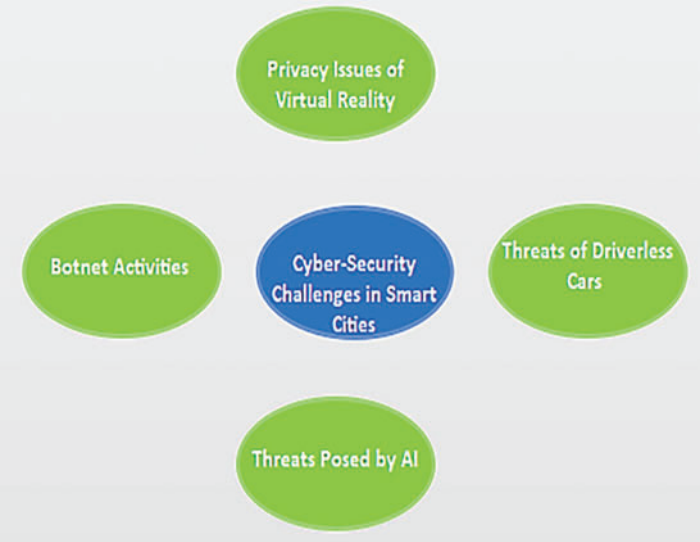

Figure 5: Cyber-security challenges in smart cities

3.1 Cyber-Security Challenges in Smart Cities

Botnet Activities in IoT-Based Smart Cities: IoT systems are increasingly targeted by newly discovered IoT botnets. The Mirai botnet stands out as a notable illustration, with the capability to infect a diverse range of IoT devices, including webcams, printers, IP cameras, DVRs, and routers [61]. Once compromised, these devices are harnessed to spread the infection and execute Distributed Denial of Service (DDoS) attacks against designated servers [62]. Unlike computers and smartphones, IoT devices often lack robust security measures or have none at all. Unfortunately, the severity of this threat only became apparent in the latter half of 2016 [63]. Consequently, significant efforts are required from the security sector to develop new defenses; otherwise, the IoT-enabled ecosystem risks being severely impacted by this new normal of DDoS assaults. Addressing these vulnerabilities is crucial to safeguarding smart city infrastructures from widespread disruptions and ensuring the reliability of essential services.

Challenges of Autonomous Vehicles in Smart Cities: Autonomous vehicles (AVs) represent a significant investment by tech giants, aiming to reduce traffic accidents and foster a more sustainable urban environment [64]. However, the potential for AVs to be compromised, endangering both personal data security and human safety, has raised substantial security concerns. Exploiting vulnerabilities, hackers can remotely manipulate AVs, including sudden braking, engine shutdown, and steering control [65]. Furthermore, the extensive collection of personal data by AV computer systems raises significant privacy issues. Securing AV technologies against cyber threats is essential to maintain user trust and safety in smart city environments.

Privacy Concerns with Virtual Reality in Smart Cities: Virtual reality (VR) technology finds extensive use in technology-driven smart cities, employed by city planning departments, healthcare providers, and engineering industries. Yet, the sharing of sensitive data with third parties, unencrypted communication between VR devices, and data stored by sensors pose risks of privacy breaches [66]. Unfortunately, in the rush to deploy these applications, both users and designers have overlooked privacy considerations. Implementing robust encryption standards and privacy-by-design principles can mitigate these risks and enhance user privacy in VR applications.

Risks Associated with AI in Smart Cities: Artificial intelligence (AI) systems are integral to many smart applications, from automated trading systems to household appliances and medical devices. However, the expanding use of AI raises security concerns. Service providers and manufacturers can exploit data mining tools to access sensitive information and analyze personal data beyond the intended scope of their services. Additionally, hackers with AI expertise can devise sophisticated attacks, potentially undermining the effectiveness of AI-based security mechanisms [67]. Understanding the training methods of machine learning-based protections, attackers may employ strategies to diminish algorithm reliability. Establishing stringent data governance frameworks and ethical AI guidelines is crucial to mitigate risks associated with AI deployments in smart city infrastructures.

Impact of Cybersecurity Risks and Privacy Challenges on Resident Trust in Smart City Developments: Residents' trust in smart city developments is significantly influenced by the cybersecurity risks and privacy challenges outlined. The vulnerability of IoT devices to botnet attacks and DDoS incidents raises concerns about the reliability of essential services and data security within smart cities. Instances of compromised autonomous vehicles, susceptible to remote manipulation and potential data breaches, further diminish confidence in the safety and privacy protections of smart transportation systems. Additionally, privacy lapses associated with VR applications and AI-driven data exploitation exacerbate residents' apprehensions regarding personal data security and privacy invasion in urban environments. Mitigating these risks through robust cybersecurity measures, transparent

governance practices, and proactive communication strategies is essential to fostering and maintaining residents' trust in the integrity and security of smart city infrastructures.

3.2 Security Requirements

The subsequent section predominantly emphasizes identifying the requisites associated with securing smart cities, considering the characteristics of IoT devices, the intricate urban environment, and the security and privacy risks previously outlined [68], as depicted in Fig. 6.

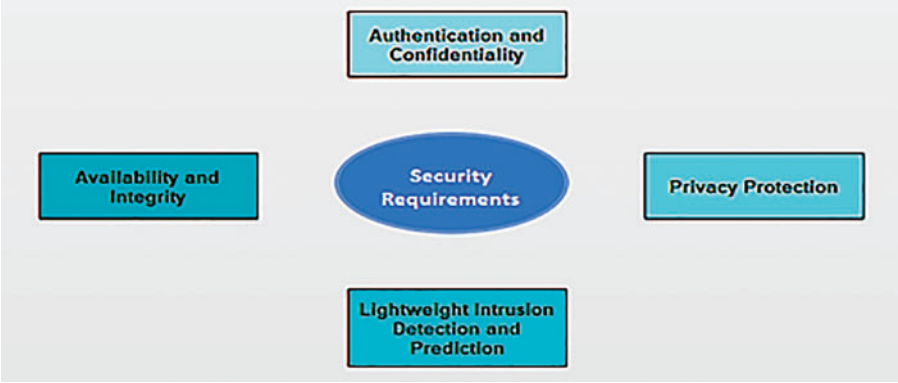

Figure 6: Security requirements for smart cities

Authentication and Confidentiality: Authentication is a fundamental necessity across all layers of a smart system, ensuring that only authorized clients access services within a diverse network by establishing identities. IoT devices play a critical role in authenticating networks, nodes, and communications within smart cities. With the rapid increase in authentication data in smart cities, it's crucial to develop advanced solutions for precise and real-time authentication [69]. Confidentiality is paramount for shielding data from hacking attempts and unauthorized disclosure. Encryption-based technologies are commonly utilized to establish secure communication and storage systems, thus safeguarding the confidentiality of information transmission between nodes. Designing identification and authentication systems presents challenges due to transparency and reliability requirements.

Availability and Integrity: Availability ensures that tools and services remain accessible when needed, even in the face of attacks. Smart systems should be capable of recognizing abnormal conditions and effectively halting additional system damage [70]. Resilience, defined as a system's capacity to withstand defects and failures resulting from attacks and disasters, is crucial. Strong and adaptive defense mechanisms are necessary to counter more intelligent attacks. Ensuring the security of IoT devices and data transferred between them and the cloud is imperative. Ensuring data integrity during transmission is a concern due to the potential risk of tampering during data exchange among multiple devices [71]. Although techniques such as firewalls and protocols regulate data traffic in IoT communications, maintaining integrity at endpoints presents challenges because of the limited computational capacity of most IoT devices.

Lightweight Intrusion Detection Techniques: Predicting and preemptively addressing risks is preferable to discovering them after an attack. Many intrusion prediction systems (IPS) fail to effectively identify and stop intrusions, as evidenced in web-based applications and smart grids [72]. Designing intelligent IPS systems to achieve security status awareness and automatically predict various attacks on smart apps is essential.

Privacy Protection: Privacy protection is intertwined with security and encompasses various security requirements. The primary cause of privacy breaches in smart city scenarios continues to be sensitive data leakage, whether intentional or unintentional. This is further compounded by common risks such as packet interception, malware, hacking, and permission falsification [73]. Effective countermeasures, including encryption techniques, anonymous mechanisms, and strategies like differential privacy, are required to prevent unauthorized usage. Privacy-preserving data mining techniques must also be employed to mitigate privacy violations. Additionally, policies, governance, and education should complement technical measures for comprehensive protection, as adopting solely technical solutions is insufficient [74].

3.3 Intrusion Detection System

The primary objective of an Intrusion Detection System (IDS) is to safeguard an information system against unauthorized access [75], which could compromise information availability, confidentiality, or integrity.

By scrutinizing network traffic or resource usage patterns, an IDS seeks to identify any signs of malicious activity and promptly issue alerts if such behavior is detected [76]. IDSs can be broadly categorized into two main classes based on their approach to intrusion detection, as depicted in Fig. 7. One category compares observed events with a database of known intrusion techniques, while the other analyzes normal system behavior and flags deviations as potential intrusions. An Intrusion Detection System (IDS) is implemented to continuously monitor traffic data with the objective of detecting and preventing intrusions that could compromise the confidentiality, integrity, and availability of an information system. The operational workflow of an IDS consists of three main phases. In the initial monitoring phase [77], network-based sensors are deployed to observe the system environment. The subsequent analysis phase incorporates algorithms for feature extraction and pattern classification, enabling the detection of anomalies and potential security breaches. Finally, the detection phase involves identifying and responding to both abnormal system behavior and suspected intrusion attempts. An IDS is designed to capture and analyze a replica of data traffic within information systems, as illustrated in Fig. 8, to identify potentially harmful activities.

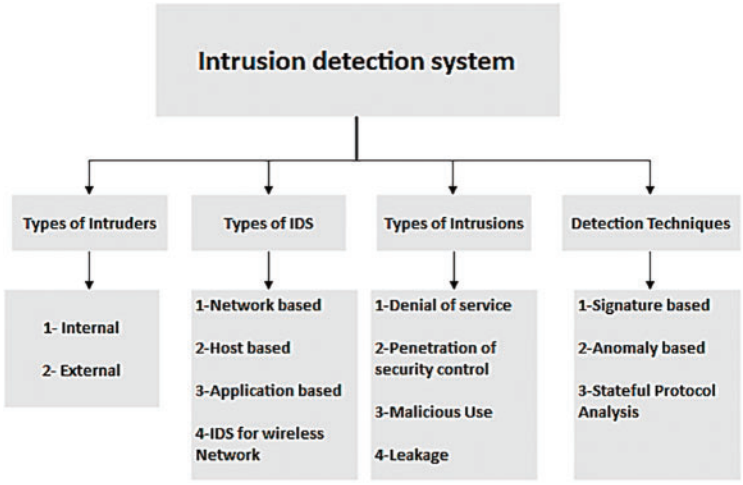

Figure 7: Types of IDS

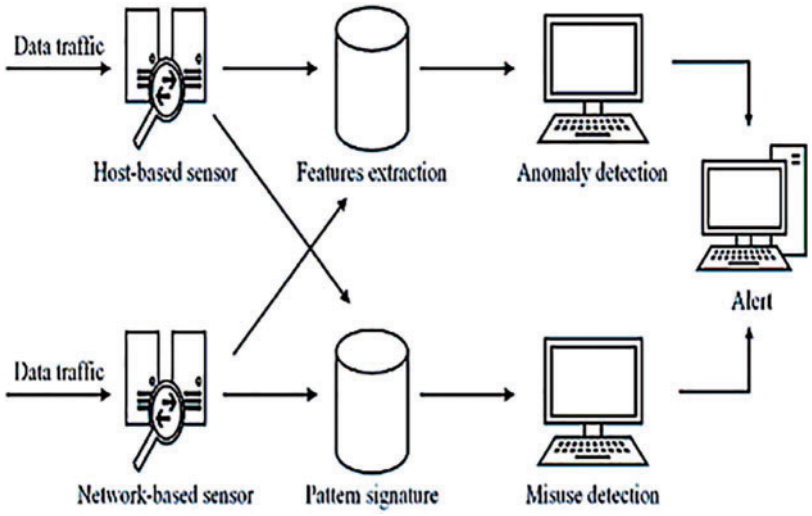

Figure 8: Mode of operation IDS

Signature-Based IDS: A signature-based IDS (SIDS) bases its detection of new threats on a database of previous attacks [78]. Using matching techniques or protocol conformance checks, the signatures of the active actions are extracted and put to the test against the signatures in the database. If a match is discovered, an alert is triggered. It is possible to monitor hosts directly in both online and offline modes, generate real-time alarms, and view system logs while doing so. Other names for this category of IDS include misuse detection and knowledge-based detection. Extraction of traffic signatures may be difficult and time-consuming, depending on the quantity of traffic aspects to be taken into account. Most of the time, signatures are manually created by professionals who have in-depth knowledge of the vulnerabilities the system is designed to catch, as part of the technique for automatically generating malicious traffic signatures [79].

Anomaly-Based IDS: SIDS issues are resolved using anomaly-based intrusion detection systems (AIDS). During the training phase, a model of the nominal behavior of AIDS is typically constructed. When implemented, a standard IDS keeps track of computers and compares them to the ideal one. An IDS alarm may be issued whenever there is a significant departure between host behavior and the model [80]. With this approach, an AIDS might be able to detect zero-day assaults since it does not assess the behavior of live hosts against those in a database. Aside from being deployed for security, AIDS can also be used as a method for system analysis. The IDS reports an anomaly when there is a change from the baseline conditions; this change could be the result of an intrusion or a logic fault in the device. An AIDS has a higher rate of false positives compared to SIDS. It is true that an AIDS may issue erroneous alarms if it is unaware that a targeted system may change its behavior while in use without any external intervention.

Network Intrusion Detection System (NIDS): The Network Intrusion Detection System (NIDS) scrutinizes all traffic originating from each device on the network at a specific location within the network [81]. It can identify and prevent attacks before they start by monitoring and comparing the traffic passing across the entire subnet to the known attack collection. After an attack or unusual activity is detected, the administrator may receive a notification [82]. On a subnet containing firewalls, NIDS can be used to determine whether they have been compromised as illustrated in Fig. 9.

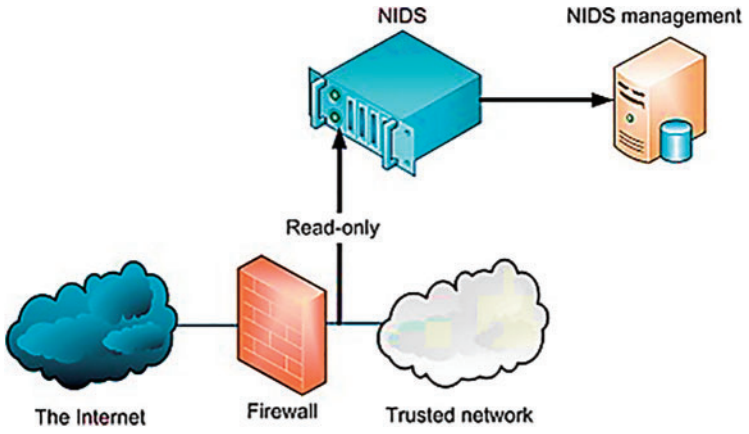

Figure 9: NIDS architecture

Host Intrusion Detection System (HIDS): It deployed on individual hosts or sensors, notifies administrators upon detecting suspicious or malicious activities. HIDS exclusively monitors incoming and outgoing packets from the device, comparing the latest snapshot with the previous one [82]. Administrators are alerted if changes or deletions occur in critical system files. For instance, HIDS is commonly applied to safeguard mission-critical machines with fixed configurations. Analysis in HIDS relies on factors extracted from the host environment, such as log files, to inform decision-making processes. The underlying principle of HIDS involves extracting features from the host environment, as depicted in Fig. 10.

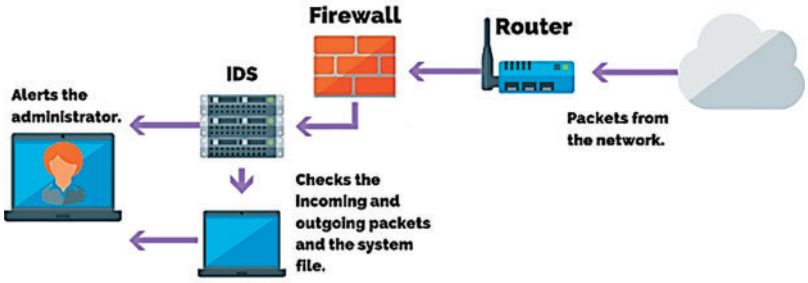

Figure 10: HIDS architecture

Application Protocol-Based Intrusion Detection System (APIDS): It operates as a system or agent situated on a server cluster, identifying attacks through analysis of communication protocols [83]. For instance, middleware might monitor SQL protocol usage to interact with a web server's database.

Hybrid Intrusion Detection System (Hybrid IDS): it merges two or more IDS methodologies, combining host agent and network data to provide a holistic network system overview [84]. Compared to standalone IDSs, the hybrid IDS demonstrates greater efficiency.

3.4 Discussion

The cybersecurity challenges outlined in the paragraph above shed light on the vulnerabilities inherent in smart cities, despite their significant technological advancements. From botnet activities targeting IoT-based infrastructures to the security threats posed by autonomous vehicles and virtual

reality technology, it's evident that the rapid expansion of smart city applications comes with its share of risks. These obstacles emphasize the essential requirement for strong security protocols to uphold the integrity of sensitive data, guarantee user privacy, and defend against cyber threats. The security requirements highlighted in the paragraph emphasize the fundamental aspects necessary for securing smart cities effectively. Authentication and confidentiality play vital roles in establishing secure identities and protecting data transmission across heterogeneous systems. Availability and integrity are equally crucial, ensuring that smart systems can continue operating effectively even under attack and withstand multiple failures. Lightweight intrusion detection techniques and privacy protection measures are essential components in proactively identifying and mitigating security risks, as they allow for the early detection of threats and the safeguarding of sensitive information.

In the next part, we will delve into existing security solutions for smart cities, examining how these solutions address the identified cybersecurity challenges and security requirements. We will evaluate their effectiveness in mitigating risks and discuss potential recommendations for enhancing smart city security further. By comprehending the present state of security solutions and pinpointing areas necessitating enhancement, we can enhance the safeguarding of the integrity, confidentiality, and accessibility of smart city infrastructure and services.

4 Existent Security Solutions within Smart Cities

In addition to identifying primary security and privacy concerns in smart cities, various studies, as highlighted by Cui et al. [85], have also put forward solutions to tackle these challenges. Smart cities are anticipated to elevate the quality of life for individuals, foster sustainable development, and streamline urban operations [86]. Amidst the proliferation of smart technologies, the spotlight has shifted toward security and privacy concerns, prompting the need for suitable remedies. Given the diverse, scalable, and dynamic nature of smart cities, not all cybersecurity measures can be universally applied to every intelligent application. When formulating and deploying new protocols or systems, it's crucial to prioritize security and privacy concerns [87]. Across the globe, cities are increasingly developing smart strategies to confront these challenges, with the goal of improving residents' quality of life, fostering economic development, and sustainably managing urban environments. China, as the world's most populous nation, is actively involved in over 200 smart city initiatives. Notably, the infrastructure of cities worldwide now encompasses billions of devices, spanning areas such as mobile mobility, smart governance, automation, and intelligent housing, all of which offer potential benefits for residents [88].

In this section, we present significant findings regarding existing and potential technologies utilized to address security and privacy challenges within the framework of smart cities. The technical illustrations employed here are drawn from diverse disciplinary perspectives.

4.1 Cryptography

Cryptographic algorithms play a pivotal role in securing smart application services by preventing unauthorized access throughout the data lifecycle, which includes storage, processing, and sharing. The aim of this section is to outline the existing cryptographic tools employed in smart systems and spotlight emerging technologies in the field. Traditional encryption standards encounter challenges when deployed on resource-constrained devices due to their computational complexity and energy consumption [89]. Encryption schemes are fundamental to maintaining data confidentiality in smart application services, ensuring that unauthorized access is thwarted at every stage of the data lifecycle, from storage to dissemination [90].

Therefore, it is essential to examine modern cryptographic techniques utilized in smart systems and emphasize specific innovative technologies. However, traditional encryption methods may not be entirely suitable for resource-constrained devices due to their computational requirements and energy consumption [91]. Thus, lightweight encryption has become crucial for practical implementation in real-world scenarios. Several studies have proposed authentication solutions for IoT environments to protect edge user communications against DDoS attacks. Moreover, novel lightweight authentication systems leveraging public key encryption have been introduced to enhance the security of smart city applications [92]. Homomorphic encryption (HE) deserves attention for its capability to perform computations on encrypted data while preserving sensitive information. This technology has garnered increasing interest due to its diverse applications, such as safeguarding electricity consumption aggregation in smart grid systems, ensuring privacy in healthcare monitoring, and addressing security concerns in cloud computing [93]. Zero-knowledge proofs offer a cryptographic technique that allows one party to demonstrate a fact to others without revealing additional information. These proofs are instrumental in addressing authentication challenges, as demonstrated in [94], where zero-knowledge proofs were used to devise an efficient authentication protocol for smart cards.

4.2 Blockchain

Although the Blockchain method is not a separate field but a technique, it has emerged as a solution to security challenges in smart cities, as shown by many studies. This is particularly noteworthy given the dramatic increase in interest in recent years. Several studies have demonstrated the potential of integrating blockchain into the IoT ecosystem, highlighting potential applications in this disruptive field.

Extensive research in this area [95] has confirmed the possibility of incorporating blockchain technology into the IoT domain, emphasizing its significant value within the evolving IoT ecosystem. Blockchain's governance structure enables applications to run in a distributed manner, which is the main driver behind the popularity of many blockchain-based IoT applications [96]. In 2019, Gong et al. [97] developed a security framework based on blockchain technology to ensure device communication security within a smart city while improving system reliability and performance. Similarly, in 2021, Ammi et al. [98] integrated blockchain technology into a smart home environment, to achieve the goals of privacy, authenticity, and availability. Although blockchain technology has received a lot of attention in recent years, leading to the development of reliable and useful applications, its use in the IoT era is still in its infancy. There is an urgent need to advance the sophistication of these technologies to effectively address critical privacy and security concerns.

4.3 Biometrics

Numerous studies within the scholarly literature have recognized biometrics as a viable remedy for confronting paramount security and privacy concerns in the context of smart cities. Biometrics finds extensive application in authenticating IoT-based systems [99], facilitating the automated verification of individuals by leveraging distinctive biological and behavioral attributes. Diverse forms of biometric data, encompassing facial features, vocal patterns, and signature dynamics, among others, are harnessed for the purpose of biometric authentication. Of particular significance is the emergence of brainwave-based authentication, which warrants attention owing to its capacity to attain a heightened level of identification reliability while concurrently preserving operational efficiency [100].

Several studies have proposed essential discussions and standard authentication protocols to safeguard users' sensitive information on storage devices. Unlike existing similar systems, the distinct

protocol not only effectively mitigates security attacks but also maintains an appropriate communication overhead. It's essential to recognize that without proper implementation of these bio-based technologies, the risk of privacy breaches may increase [101]. Moreover, the development of privacy-preserving biometric techniques is imperative. Researchers have also suggested that biometrics hold promising prospects in various other sectors, including e-commerce.

4.4 Machine Learning

Machine learning techniques have been effectively utilized to bolster the efficiency of intrusion detection systems, rendering them indispensable cybersecurity tools for safeguarding networks against real-world attacks [102]. The increasing popularity of wireless sensor networks, which are integral to smart environments, has further underscored the relevance of machine learning in fortifying security measures. A comprehensive examination has elucidated the diverse advantages of employing machine learning technology to fortify smart cities, encompassing a range of ML techniques [103]. Additionally, recent research has introduced a machine-based approach for securely sensing and fusing information in wireless sensor networks (WSNs). Moreover, innovative methods for feature extraction and model selection have been devised to accurately detect attacks in Wi-Fi systems [104]. Various consumer-oriented ML techniques have been deployed to evaluate, forecast, and personalize security solutions. Despite the advancements, the subjectivity of user data used for analysis may pose challenges in accurately reflecting reality across diverse IoT environments [105]. It's important to note that ML technologies hold significant potential for enhancing various defense strategies. For example, Zhu et al. [106] proposed a game-theoretic model leveraging ML to identify and counter intrusions in wireless sensor networks (WSNs). Furthermore, Rawal et al. [107] conducted a comprehensive review of existing biometric security systems, with a particular focus on adversarial ML perspectives.

4.5 Game Theory

Game theory, a robust mathematical framework, has demonstrated remarkable effectiveness in tackling cybersecurity and privacy concerns across various scenarios [108]. In a comprehensive survey conducted by Zhu et al. [109], the unique attributes of game-theoretic approaches and their advantages over traditional defense mechanisms were delineated. The increasing interest in utilizing game theory to confront security and privacy challenges in IoT-based applications has become apparent in recent years. For example, Gill et al. [110] introduced innovative attack analysis strategies for cloud storage using evolutionary game theory. In a recent study, Li [111] delved into the realm of low-powered devices, proposing a novel lightweight anomaly detection method that ensures both precision and minimized energy consumption. Additionally, Shi et al. [112] developed a game-theoretic framework aimed at analyzing the intricacies of attack and defense mechanisms in honeypot-enabled networks, with a particular focus on communication security. This adaptable model holds promise for integration into emerging IoT landscapes, including those in smart healthcare, infrastructure, and sensor networks. While the direct application of game theory in specific smart city contexts may be limited, the domain of IoT security has experienced significant technological advancements. With the rapid evolution of interconnected smart cities, it is anticipated that game-theoretic methodologies will play a crucial role in addressing novel security and privacy challenges in this era of intelligent technologies.

4.6 Ontology

Ontology, a significant branch of philosophy, emerges as a promising tool for addressing various issues, particularly those related to unstructured data, knowledge, and configurable systems. Its primary goal is to improve comprehension, description, and reuse of formally represented knowledge,

thereby facilitating the discovery of new insights and the identification of inconsistencies. These inherent characteristics have spurred numerous ontology-based initiatives aimed at addressing security and privacy challenges, including cyber-attack detection and security risk management [113]. However, the utilization of ontology in the IoT domain remains relatively new, with only a few recent endeavors in this area. For instance, Tao et al. [114] introduced an innovative ontology-based security management model for smart homes, enhancing interaction efficiency among smart devices and bolstering system security. Similarly, Shahzad et al. [115] proposed an ontology-driven security analysis framework for smart homes, simplifying the automatic capture of consistencies during interactions. Recognizing the pivotal role of mobile phones in smart cities, Onu [116] developed an ontology-based model to characterize and manage users' personalized and dynamic privacy-control patterns in mobile computing environments. However, a significant limitation of current ontology-based studies in IoT security is their focus on specific application scenarios or requirements, lacking a unified model that diminishes their practical value. To tackle this challenge, Iqbal et al. [117] proposed a semantic-ontology-based situation reasoning method in 2022. This method provides a more comprehensive perspective on security situations while enhancing emergency response capabilities.

4.7 Non-Technical Supplements

Relying solely on technical solutions proves inadequate for comprehensive protection. Addressing the limitations of existing technology necessitates reinforcing related policies, regulations, governance, and educational efforts [118]. From a governance and political perspective, establishing robust governance is essential for constructing a trustworthy smart system. Christofi [119] emphasized the necessity of government regulations to safeguard data and model development within the framework of smart cities. Training initiatives aimed at enhancing the skills of manufacturers, service providers, and end-users are of paramount importance. For example, application designers should undergo training to foster robust and resilient coding practices. Vendors bear the responsibility of regularly updating firewalls to address vulnerabilities. Furthermore, device manufacturers should strive to enhance overall safety and quality standards to the greatest extent possible. Education programs play a crucial role in augmenting citizens' understanding of smart applications and empowering them to protect themselves [120]. However, ensuring the effectiveness of these programs poses a challenge. Barth et al. [121] discovered that although some users are aware of the potential risks of privacy breaches, they often prioritize convenience over these concerns.

4.8 Risk Management and Virtualization

The risk management is considered as a key solution for handling cyber security issues within smart cities. It basically consists in identifying cyber threats, assessing their risks and setting up mitigation strategies. As example, the authors in [122] proposed a novel approach for a dynamic cyber security risk management within e-health systems considered as main applications within smart city environments. From another perspective, virtualization offers a good opportunity to enhance the flexibility of smart applications. As they allow a high level of flexibility, software defined networks (SDN) and network virtualization functions (NFV) promote the development of smart city infrastructures while other security issues are associated to the use of those technologies. To address these challenges, several research works are conducted like the work proposed in [123] for enhancing intrusion detection within SDN/NFV-based smart city infrastructures.

4.9 Discussion

The current landscape of smart cities is characterized by a myriad of security and privacy concerns, prompting extensive research efforts to identify and address these challenges. Various studies have not only pinpointed these issues but have also proposed solutions to mitigate them. Smart cities, envisioned to enhance the quality of life, promote sustainability, and optimize urban processes, are increasingly focusing on security and privacy amidst the proliferation of smart technologies. However, the diverse, scalable, and dynamic nature of smart cities poses challenges in applying universal cybersecurity measures to every intelligent application. As cities worldwide formulate their smart strategies to tackle these challenges, it's evident that the infrastructure of modern cities spans billions of devices, offering potential benefits but also raising security and privacy concerns.

In this section, we have presented a recap of proposed solutions, such as how cryptographic algorithms establish the bedrock for security and privacy measures in smart application services, thwarting unauthorized access across the data lifecycle. However, conventional encryption methods face challenges in resource-constrained devices, necessitating lightweight encryption for practical implementation. Emerging technologies like homomorphic encryption and zero-knowledge proofs offer innovative solutions to address authentication and privacy concerns. Blockchain technology has surfaced as a promising remedy for security challenges in smart cities, as evidenced by several studies underscoring its viability and utility within the IoT ecosystem. Security frameworks based on blockchain have been proposed for ensuring communication security and confidentiality in smart home settings. Biometric authentication offers a promising solution for addressing security challenges in smart cities, enabling autonomous identification based on biological and behavioral traits. However, the implementation of bio-based technologies requires careful consideration to mitigate privacy risks. Machine learning techniques boost the effectiveness of intrusion detection systems, which serve as pivotal cybersecurity infrastructure for safeguarding networks against attacks. These techniques offer various benefits for safeguarding smart cities, including improved accuracy in attack detection and personalized security solutions. Game-theoretic approaches have gained traction in addressing security and privacy challenges in IoT-based applications. These methodologies offer advantages over traditional defense mechanisms and hold promise for enhancing security in emerging IoT landscapes. Ontology-based initiatives address security and privacy challenges by enhancing understanding and description of knowledge in smart systems. However, current efforts lack a unified model, limiting their practical value in IoT security. Non-Technical Supplement which Relying solely on technical solutions is insufficient for comprehensive protection. Strengthening related policies, regulations, governance, and educational efforts is crucial for addressing the limitations of existing technology and enhancing cybersecurity resilience in smart cities.

Despite the progress made in existing security solutions, threats to smart cities persist, necessitating ongoing research and innovation to develop more effective protection measures. In the face of evolving technology, continuous vigilance and adaptation are essential to safeguarding smart cities from emerging threats. In the subsequent discussion, we propose our approach for protecting smart cities, focusing on intrusion detection and offering a detailed examination of our methodology.

Furthermore, in this detailed discussion, we have highlighted various cutting-edge technologies and strategies aimed at mitigating security and privacy challenges in smart cities, as outlined in the section on '4 Existent Security Solutions within smart cities.' These insights underscore the ongoing efforts and advancements in smart city security, emphasizing the need for continuous innovation and adaptation to effectively safeguard urban environments from evolving threats.

5 Proposed Approach

5.1 Objectives and Principle

Our preceding sections meticulously delved into the myriad security risks inherent in smart cities, underscoring the pervasive nature of these vulnerabilities across all facets of urban infrastructure. The interconnectedness of various components within smart cities amplifies the significance of safeguarding against cyber threats, necessitating a holistic approach to fortify defenses. In response to this imperative, we propose a multifaceted strategy aimed at mitigating the diverse array of cyber security challenges facing smart cities. Central to our solution is the meticulous analysis of data sourced from an extensive array of devices embedded within the urban landscape. By harnessing the wealth of information generated by these interconnected devices, our strategy enables a proactive and data-driven approach to identifying and neutralizing potential threats in real-time. By harnessing sophisticated analytics and machine learning algorithms, we can unveil concealed patterns, anomalies, and signs of compromise that might elude conventional security measures. Furthermore, our comprehensive strategy extends beyond mere detection and response, encompassing proactive measures such as threat intelligence sharing, security awareness training, and robust incident response protocols. By fostering collaboration and information sharing among stakeholders, our approach fosters a culture of collective vigilance and resilience against emerging cyber threats. Ultimately, through the implementation of our holistic strategy, smart cities can fortify their cyber defenses and safeguard the integrity, confidentiality, and availability of critical infrastructure and services for the benefit of all residents and stakeholders.

Henceforth, the overarching aim of our strategic framework is to proactively detect, mitigate, and thwart infiltration attempts within smart cities. Employing the following functionalities will facilitate the realization of this objective: Firstly, leveraging automated learning methodologies to detect infiltration attempts and discern their characteristics and severity levels accurately. Secondly, tracking identified intrusions and precisely determining their origins and locations, thereby enhancing awareness of the security posture of smart city components. Our strategy's ultimate objective is to preemptively halt intrusion endeavors at their inception. This framework utilizes formal methodologies and artificial intelligence to achieve the following objectives: (i) thoroughly document penetration attempts, modifications, and cyberattacks to promptly detect any deviations from security standards; (ii) monitor malicious behaviors and accurately trace their sources; and (iii) establish strong controls to effectively repel and prevent such threats.

5.2 Approach Architecture

Our system adopts a layered architecture with a modular design, comprising three fundamental subsystems: HIDS (Host Intrusion Detection System), NIDS (Network Intrusion Detection System), and SPIDS (Storage and Processing Intrusion Detection System). The core unit of the system, known as the MONITORING CENTER, serves as a central unit, as illustrated in Fig. 11 below.

Host Intrusion Detection System (HIDS): Regarded as a primary decision-maker at the initial level, this subsystem oversees intrusion detection management within the data acquisition layer. It maintains its repository housing relevant datasets pertaining to the devices stationed within the monitoring center. The HIDM assesses data originating from the generating nodes (devices), scrutinizes node behavior, and subsequently relays it to the MC, as depicted in Fig. 11.

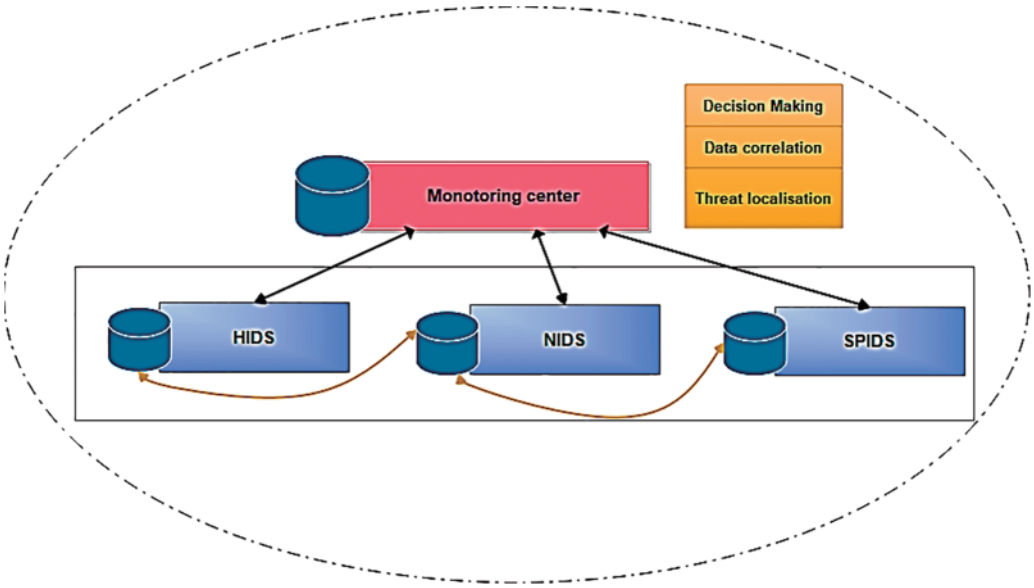

Figure 11: Monitoring center for cybersecurity in smart cities

Network Intrusion Detection System (NIDS): This subsystem also operates at the initial level of the decision-making process. Its function is to recognize behaviors associated with the communication channels utilized within the smart city. In the event of abnormal traffic, communication may be interrupted. Subsequently, logs and analyses are transmitted to the MC.

Storage and Processing Intrusion Detection System (SPIDS): It constitutes the third unit within the comprehensive system management framework, concerning the data storage and processing subsystem. The outcomes derived are likewise relayed to the MC.

MC (Monitoring Center): The primary module responsible for executing end-to-end intrusion management is referred to as the MC (Monitoring Center). This component acts as an orchestrator, overseeing the workflow among the other modules. A centralized database stores the information collected from these modules. Initial thresholds are communicated to the subsystems, which are then updated based on the gathered data. The system can either provide periodic updates or dynamically adjust thresholds based on the system's monitored performance. One of the MC's key responsibilities is correlating results. The Monitoring Center operates at various levels within smart cities, as depicted in Fig. 12.

The monitoring center acts as a central nexus tasked with gathering information from diverse nodes spanning across different tiers of a smart city infrastructure. This encompasses contextual data sourced from various points within the urban landscape. Once collected, the data undergoes thorough analysis, incorporating reports and historical data to gain insights. Subsequently, the center generates reports based on this analyzed data, encompassing various types such as threat evaluation, threat response monitoring, threat management, and threat analysis and classification.

Centralized Data Collection: The monitoring center acts as a centralized entity to gather information from diverse sources within the smart city ecosystem. This centralized approach enables efficient data collection and management.

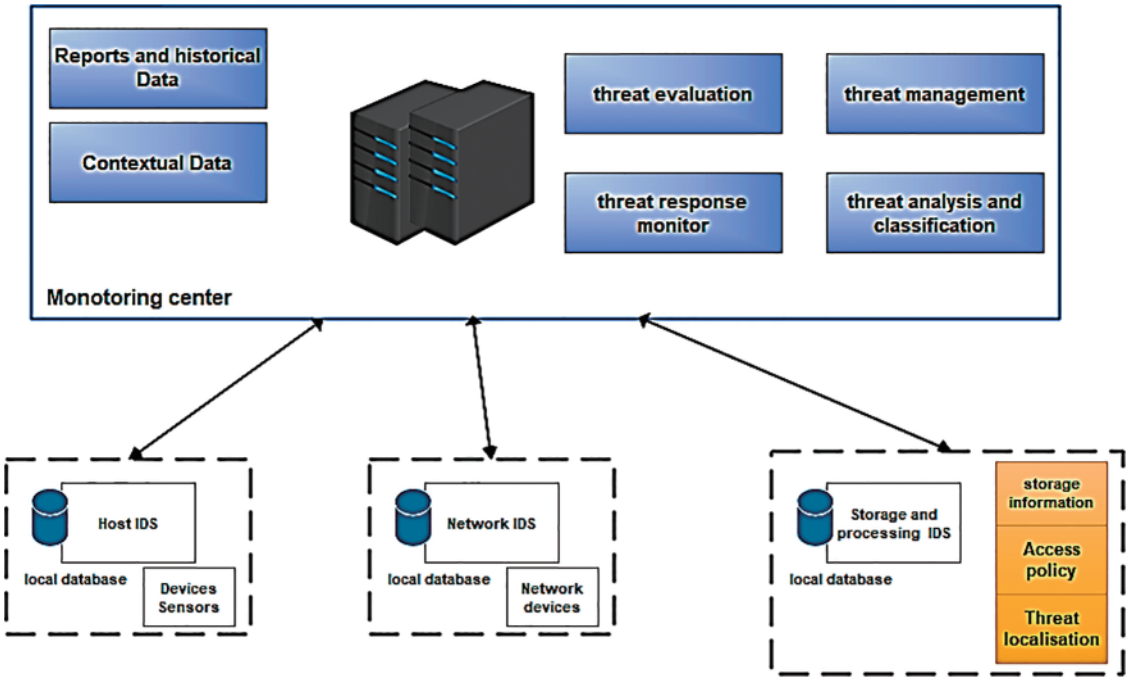

Figure 12: Different level for monitoring center in smart cities

Contextual Data Analysis: The center conducts analysis on the amassed data, encompassing contextual details from multiple source of the smart city infrastructure. This analysis entails detecting patterns, trends, anomalies, and potential threats embedded within the data.

Utilization of Reports and Historical Data: In addition to real-time data, the analysis incorporates reports and historical data. This historical context provides valuable insights into past occurrences, trends, and responses, enhancing the quality and accuracy of the analysis.

Report Generation: Based on the analysis, the monitoring center generates various types of reports. These reports serve different purposes, such as evaluating threats, monitoring responses to threats, managing ongoing threats, and analyzing and categorizing different types of threats. This methodical approach enables informed decision-making and proactive responses to mitigate potential risks and challenges in the smart city landscape. The suggested architecture primarily relies on fundamental modules (HIDM, NIDM, and SPIDM), each functioning as independent intrusion agents. They assess and analyze behavior associated with individual layers, making decisions autonomously, as depicted in Fig. 13.

5.3 Case Study

In Fig. 14, we introduce a methodology tailored for detecting cyber threats within IoT-driven smart cities. This proposed approach lays the foundation for employing machine learning techniques like logistic regression, decision trees, random forest, KVM (Kernelized Vector Machines), and SVM (Support Vector Machines) to identify potential attacks and malicious activities in forthcoming urban IoT networks. Logistic regression, a statistical tool, is adept at binary classification, estimating the likelihood of a specific class. Decision trees, which are non-parametric supervised learning methods, find utility in both classification and regression tasks. Random forests, an ensemble learning technique,

construct multiple decision trees and generate the mode of classes (classification) or the mean prediction (regression) from the individual trees. KVM, or Kernelized Vector Machines, represent a category of supervised learning algorithms for data analysis and pattern recognition, applicable to classification and regression tasks. SVM, or Support Vector Machines, constitute another class of supervised learning algorithms utilized for classification and regression analysis. Our approach operates under the assumption that monitoring network traffic at fog nodes is more effective for detecting normal and abnormal activities, given their proximity to IoT sensors compared to the vast cloud storage resources within the city. Upon identifying risks at the Monitoring Center (MC), the framework promptly notifies Host Intrusion Detection and Mitigation (HIDM) services for immediate system updates, as depicted in Fig. 14. In our IoT environment, we leverage these machine learning models to enhance security measures. By employing logistic regression, decision tree, random forest, KVM, and SVM, efficient classification software can be developed, although there are also other promising security solutions utilizing these machine learning paradigms [124].

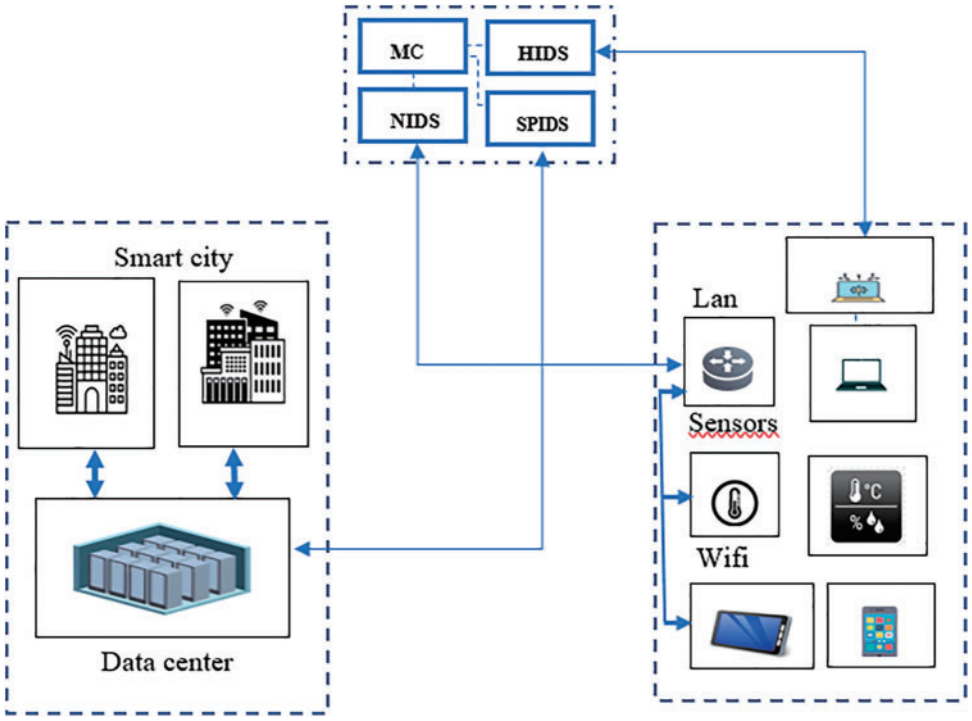

Figure 13: Layers for our approach

5.3.1 Edge-IIoTset Dataset

We employed the Edge-IIoTset [125], an innovative and comprehensive cybersecurity dataset specifically designed for IoT and IIoT applications. This dataset is well-suited for training machine learning-based intrusion detection systems and supports two learning modes: centralized and federated learning. The testbed comprises seven distinct layers: Cloud Computing, Network Functions Virtualization, Blockchain Network, Fog Computing, Software-Defined Networking, Edge Computing, and IoT and IIoT Perception. Each layer incorporates cutting-edge solutions customized to meet the specific requirements of IoT and IIoT applications.

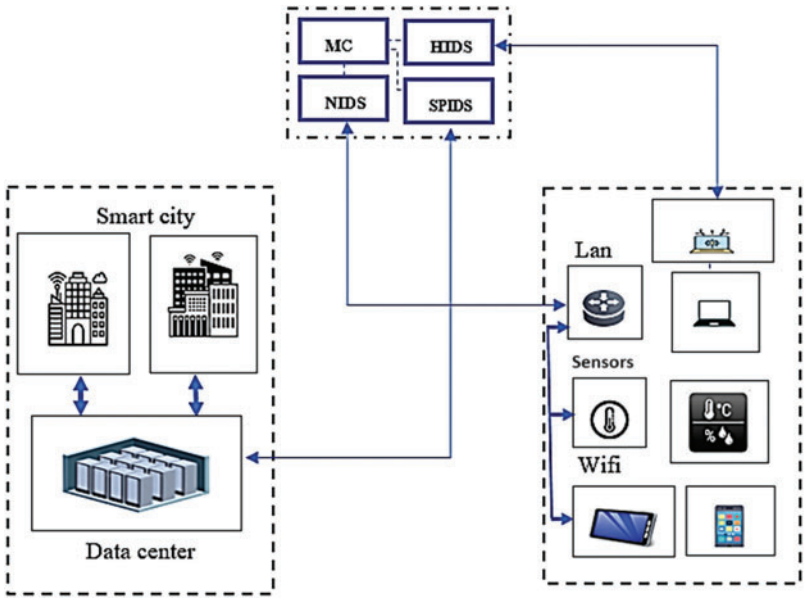

Figure 14: Proposed approach for detection system for HIDM and NIDM

These solutions include platforms such as ThingsBoard for IoT, OPNFV for network virtualization, Hyperledger Sawtooth for blockchain networks, Digital Twin technology, ONOS SDN controller for software-defined networking, Mosquitto MQTT brokers for messaging, and Modbus TCP/IP for industrial communication. The dataset utilized in our simulation involves more than ten types of IoT devices generating diverse IoT data, including low-cost digital devices, as illustrated in Fig. 15. The dataset encompasses a multitude of attacks and threats directed at IoT and IIoT application.

5.3.2 Evaluation Metrics

When evaluating the system's capability to detect botnet attacks, essential metrics such as accuracy, recall, precision, and F1-score were considered. These metrics are crucial for assessing the efficiency and effectiveness of the detection system. Their definitions are outlined as follows [126]:

$$
\begin{aligned}
accuracy &= \frac{TP + TN}{FP + FN + TP + TN} * 100\%, \\
precisioon &= \frac{TP}{TP + FP} * 100\%, \\
F1 - score &= 2 * \frac{precision * sensitivity}{precisin + sensitivity} * 100\%, \\
sensitivity &= \frac{TP}{TP + FN} * 100\%, \\
recall &= \frac{TP}{TP + FN} * 100\%
\end{aligned}
\tag{1}
$$

In this context, TP signifies true positives, FP represents false positives, TN indicates true negatives, and FN denotes false negatives.

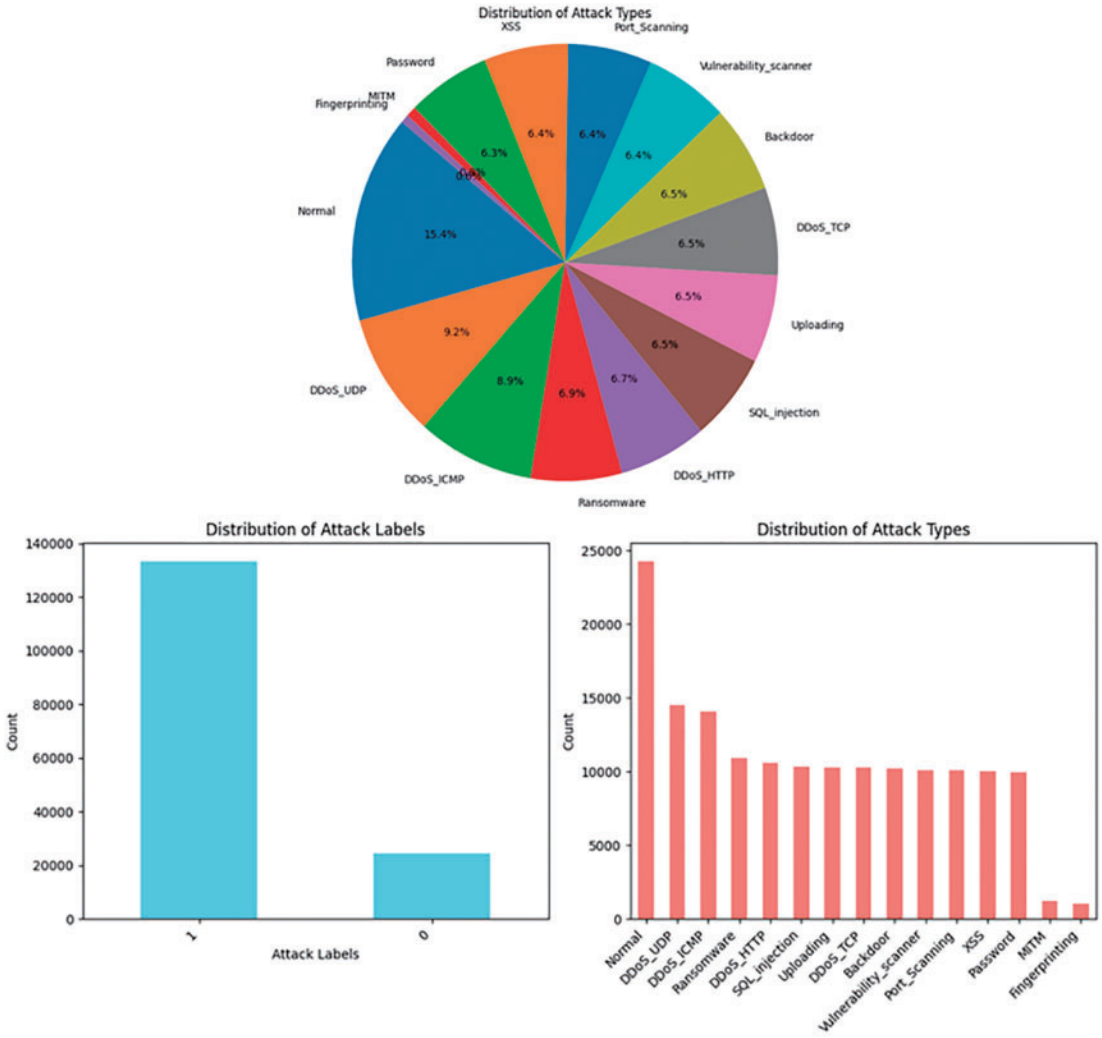

Figure 15: Distribution of attack labels and types

5.3.3 Data Transforming and Normalization

The dataset employed contains binary, continuous, and symbolic values. Since many classifiers only handle numeric values, it is essential to conduct a conversion process to ensure the effectiveness of the IDS. Of particular importance is the conversion of symbolic features. To tackle this, each distinct value is replaced with an integer. Additionally, normalization is utilized to scale features into a normalized range. In our research, we employ "one hot encoding," a simple technique, to transform classification values into binary representations.

5.3.4 Sample Attribute Normalization

Normalizing the sample data serves the purpose of facilitating cross-operation between sample attributes and understanding the correlation between different attributes. Its objective is to ensure that data with varying orders of magnitude within the dataset are mapped to a consistent scale. After

the conversion of sample attributes to numerical types, all characteristics on each data record become numerical.

The difference in value ranges among attributes significantly affects the decision-making process of the neural network model during training, especially with regard to continuous numerical features. Thus, it is crucial to normalize all continuous numerical properties to mitigate this impact and ensure the efficacy of the model. The sample attributes' normalization procedure is as follows: there are a set of data $x = \{ x_1, x_2,..., x_n\}$, in which the maximum and minimum values are x_{max} and x_{min}, respectively. Suppose that x_i is the normalized value, the calculation is as follows:

$$x_i = \frac{x_i - x_{min}}{x_{max} - x_{min}} x \in [x_{min}, x_{max}] \; i \in [1, n] \tag{2}$$

The value range of x_i calculated by (2) is mapped to numbers between 0 and 1.

5.4 Results and Discussion

5.4.1 Dataset

In this section, we detail the outcomes derived from the experiments carried out on the proposed machine learning edge IIoT dataset. The initial stage in employing machine learning involves data preparation and cleansing, which entails eliminating duplicates and handling missing values like NaN or 'INF'. Moreover, redundant features such as IP addresses, ports, timestamps, and payload details are excluded. Categorical attributes are transformed into numerical values, and feature scaling is performed using a standardization technique. Subsequently, the dataset is partitioned into training and testing subsets to facilitate model training, validation, and assessment. The statistical characteristics pertaining to normal and attack data within the dataset are outlined in Fig. 15.

The dataset provides valuable insights into network security, particularly in distinguishing between normal and abnormal activities. In analyzing the 'Attack Label Counts', it's evident that the dataset comprises a significant proportion of abnormal activities, constituting approximately 84.6% of the total observations. Conversely, normal activities make up only 15.4% of the dataset as shown in the Fig. 16. This stark contrast underscores the prevalence of potentially malicious activities within the network traffic data. Further delving into the specific types of attacks, the 'Attack Type Counts' elucidate the diverse array of threats encountered.

Notably, the most prevalent attack types include DDoS_UDP, DDoS_ICMP, and Ransomware, each posing distinct risks to network integrity and security as shown in the Fig. 16. Additionally, the presence of SQL injection, Uploading, and XSS attacks underscores the multifaceted nature of cybersecurity threats, spanning various vectors and methodologies. Visual representation of these findings through a pie chart accentuates the predominance of abnormal activities, with abnormal labels dominating the dataset.

5.4.2 Data Preprocessing

Data preprocessing stands as a pivotal phase in any machine learning pipeline, focused on refining and restructuring raw data into a format conducive to model training. An integral part of this process entails managing missing data and eliminating duplicate entries to uphold the integrity and quality of the dataset. Through techniques like isnull().sum() and duplicated().sum(), one can identify instances of missing values and duplicated rows. Respectively, missing data can skew analysis and model

performance, necessitating either imputation or removal based on contextual relevance. Similarly, duplicated rows can bias analysis outcomes, underscoring the significance of their elimination.

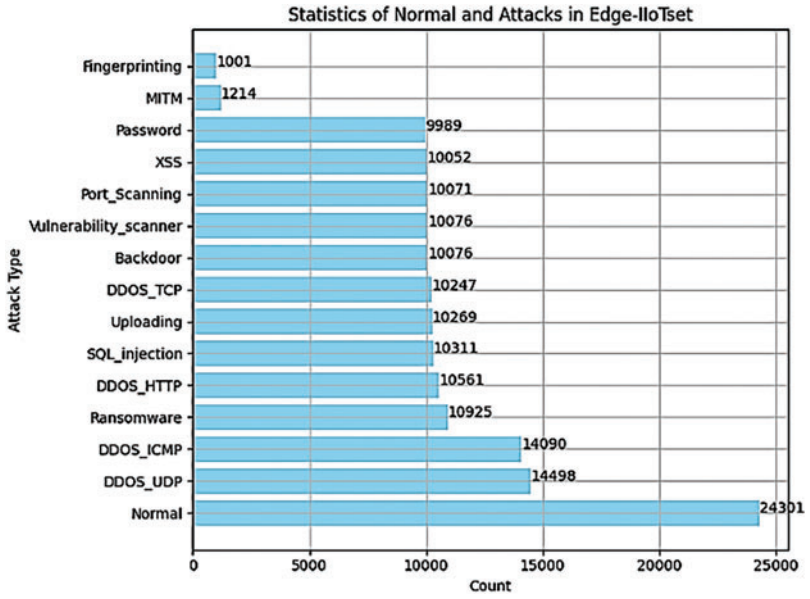

Figure 16: Statistics of normal and attacks in Edge-IIoTset

Moreover, in datasets featuring non-numerical categorical variables like 'type_attack', preprocessing entails converting these labels into a numerical format interpretable by machine learning algorithms. Label encoding, a common technique facilitated by libraries such as scikit-learn, assigns a unique integer to each category. For instance, labels like 'SQL_injection', 'Port_Scanning', 'XSS', etc., can be transformed into corresponding numerical values (e.g., 'SQL_injection' encoded as 0, 'Port_Scanning' as 1, and so forth) using the LabelEncoder function. This conversion enables effective data processing, as machine learning algorithms typically operate with numerical inputs.

In our approach, we diligently ensured the reliability and generalization of our machine learning model through rigorous data splitting techniques. Partitioning the dataset into distinct training and testing subsets is crucial for unbiased model evaluation. We allocated 25% of the data for testing purposes to ensure robust evaluation, with the remaining 75% dedicated to model training. This division strategy facilitates substantial model training while preserving a sizable portion for unbiased evaluation. Furthermore, to enhance model effectiveness and mitigate issues stemming from disparate feature scales, we employed the RobustScaler function. This preprocessing step scales dataset features using robust statistics resilient to outliers. By standardizing data into a consistent scale, RobustScaler ensures that our model can learn effectively without undue influence from outliers or variations in feature magnitudes. This meticulous preprocessing approach is instrumental in optimizing model performance and fostering reliable predictions across diverse datasets and real-world contexts.

5.4.3 Binary Classification

a) Logistic Regression

Logistic regression stands as a foundational statistical technique employed for binary classification tasks within the realms of machine learning and statistics [127]. In our model assessment, logistic

regression was utilized to scrutinize our dataset, yielding notable performance metrics: Accuracy: 0.894, Sensitivity: 0.996, Precision: 0.891, F1-score: 0.941, and Recall: 0.996. These metrics underscore the logistic regression model's efficacy in accurately categorizing instances. Moreover, Fig. 17 offers a visual representation of our analysis, portraying the model's performance comprehensively. Additionally, to provide a detailed insight into the model's predictions vis-à-vis the actual labels, we generated a confusion matrix. This matrix furnishes a granular breakdown of the model's predictive outcomes, enhancing our understanding of its classification capabilities.

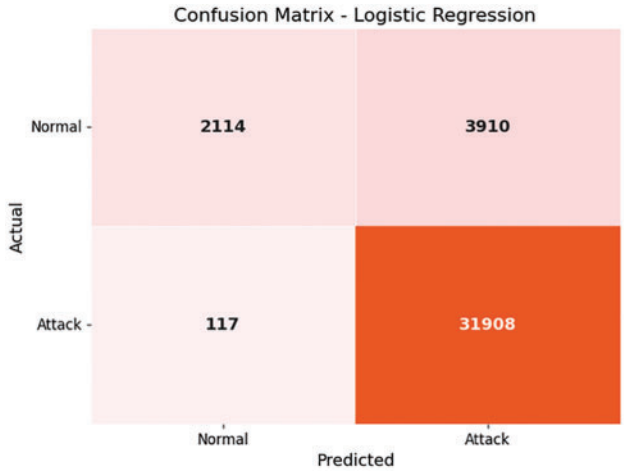

Figure 17: Confusion matrix for logistic regression

The predictive performance of our logistic regression model is demonstrated by its Receiver Operating Characteristic (ROC) curve analysis, resulting in an Area Under the Curve (AUC) value of 0.87. This indicates the model's effectiveness in discerning between positive and negative instances across various threshold settings. The ROC curve portrays the trade-off between the true positive rate (sensitivity) and the false positive rate (1 specificity), highlighting the model's ability to correctly identify true positives while minimizing false positives as shown in the Fig. 18.

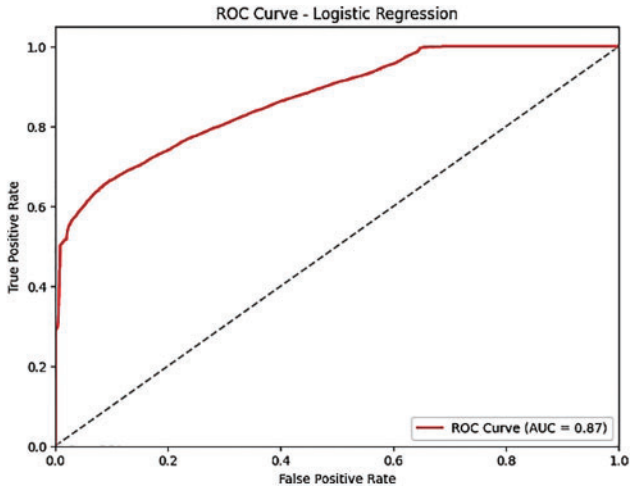

Figure 18: ROC curve for logistic regression

b) Decision Tree Classifier

The decision tree classifier stands out as a potent algorithm in supervised learning, adeptly handling tasks from classification to regression. Its methodology involves recursively segmenting the feature space into regions based on feature values, aiming to minimize impurity within each region [128]. Decision nodes in the tree correspond to partitions, while final predictions are made at the leaf nodes. In our assessment, we fine-tuned the decision tree classifier using specific parameters to optimize its performance. By setting a maximum depth of 4 and limiting features to 6, we aimed to balance complexity and prevent overfitting while capturing pertinent data patterns. Our evaluation yielded promising results: The decision tree classifier achieved an accuracy of 0.968, showcasing its proficiency in accurately classifying instances. Notably, sensitivity, representing the true positive rate, reached an impressive 0.992, indicating the model's effectiveness in identifying positive instances. Precision, reflecting the ratio of true positive predictions to total predicted positives, stood at 0.97, underscoring the model's precision in positive predictions. The F1-score, a combination of precision and recall, attained 0.981, signifying a balanced performance. Moreover, the ROC AUC, a metric indicating the model's ability to distinguish between classes, attained a commendable value of 0.958, highlighting its discriminative power. To provide a comprehensive understanding of the model's performance, we conducted a thorough analysis, including examining the confusion matrix and the ROC curve. while specific figures are not included in this text, this analysis encompassed visualizing the model's performance across different classes and understanding the trade-off between sensitivity and specificity at various classification thresholds. Overall, our evaluation demonstrates the Decision Tree Classifier's effectiveness in accurately classifying instances, with robust performance across multiple evaluation metrics, as illustrated in Fig. 19. These findings underscore the utility of decision trees as versatile and interpretable tools for predictive modeling tasks.

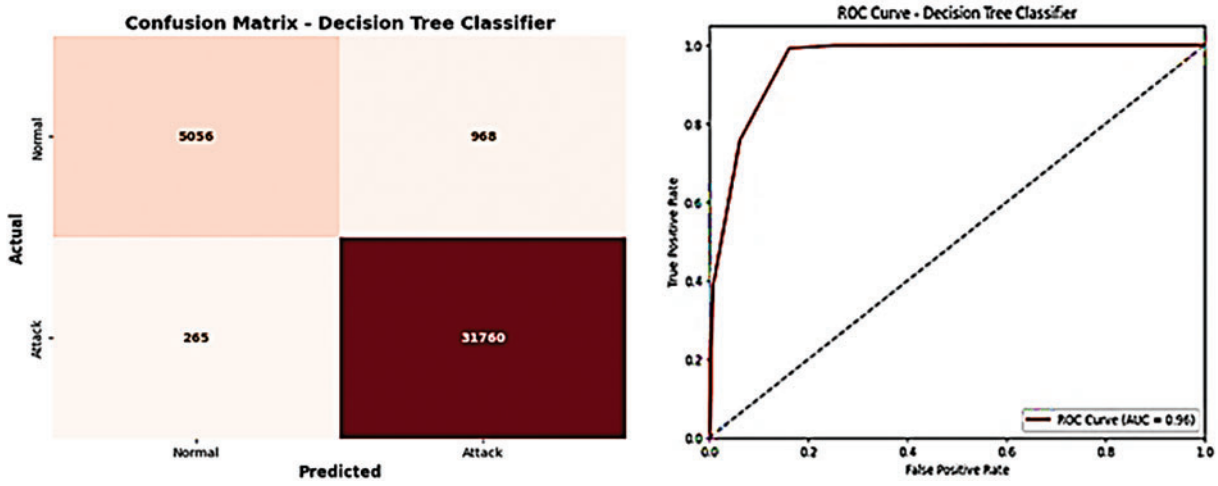

Figure 19: Confusion matrix and ROC curve for decision tree classifier

c) Random Forest Classifier

In our assessment, we opted for the random forest classifier, a robust ensemble learning technique widely employed in classification tasks [129]. The essence of the random forest lies in aggregating predictions from multiple decision trees to enhance the overall accuracy and resilience of the model. Each decision tree within the ensemble is trained on a random subset of the data and features, fostering diversity and reducing correlations among trees. For our analysis, we utilized the random forest

classifier, exploring various values for the "max_depth" parameter, which governs the maximum depth of each tree in the forest. Our investigation spanned depths from 1 to 11, aiming to identify the optimal configuration for our model. The outcomes of our evaluation revealed exceptional performance across diverse metrics: The random forest classifier achieved flawless accuracy, sensitivity, precision, F1-score, and ROC AUC, all registering a perfect score of 1.0. These metrics attest to impeccable classification performance, with the model adeptly discerning between classes. While specific figures are omitted here, we provided visual representations of our model's performance in Fig. 20, showcasing both the confusion matrix and the ROC curve. The confusion matrix offers a granular view of the model's predictions across different classes, while the ROC curve illustrates its ability to strike a balance between sensitivity and specificity across various thresholds. Overall, the Random Forest Classifier exhibited outstanding performance in our evaluation, highlighting its versatility and reliability in classification tasks. Its capacity to handle intricate datasets and deliver robust predictions positions it as a valuable asset across a broad spectrum of applications.

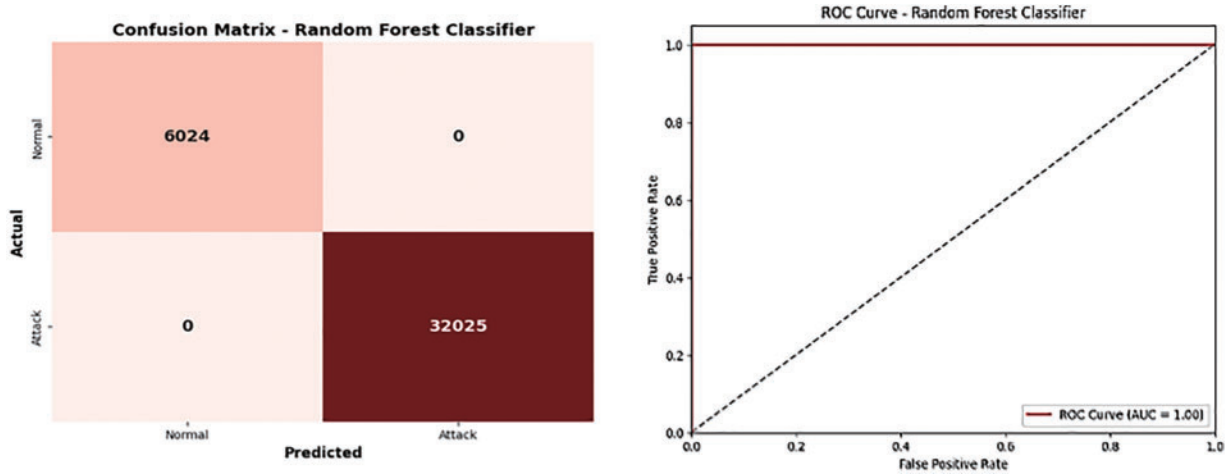

Figure 20: Confusion matrix and ROC curve for random forest

d) KNN-Model

In our assessment, we opted for the K-Nearest Neighbors (KNN) model, a widely used non-parametric classification algorithm in both supervised and unsupervised learning tasks [130]. The KNN algorithm's essence lies in its straightforward approach to classification, which relies on the majority class of the nearest neighbors in the feature space to classify new instances. For our analysis, we employed the KNN model, specifying the parameter "n_neighbors" to determine the number of nearest neighbors considered when making predictions. We set this value to 6 for evaluating the model's performance. The results of our evaluation revealed excellent performance across various metrics: The KNN model attained high accuracy, sensitivity, precision, F1-score, and ROC AUC, with values of 0.997, 0.998, 0.999, 0.999, and 0.999, respectively. These metrics highlight the model's efficiency in precisely classifying instances and distinguishing between different classes. Though specific figures are not detailed here, we included visual representations of our model's performance in Fig. 21, illustrating both the confusion matrix and the ROC curve. The confusion matrix provides insights into the model's predictions across different classes, while the ROC curve demonstrates its ability to balance sensitivity and specificity across various thresholds. In summary, the KNN model showcased outstanding performance in our evaluation, highlighting its prowess as a simple yet potent algorithm

for classification tasks. Its capacity to make predictions based on instance similarities renders it particularly valuable in scenarios characterized by complex or non-linear data distributions.

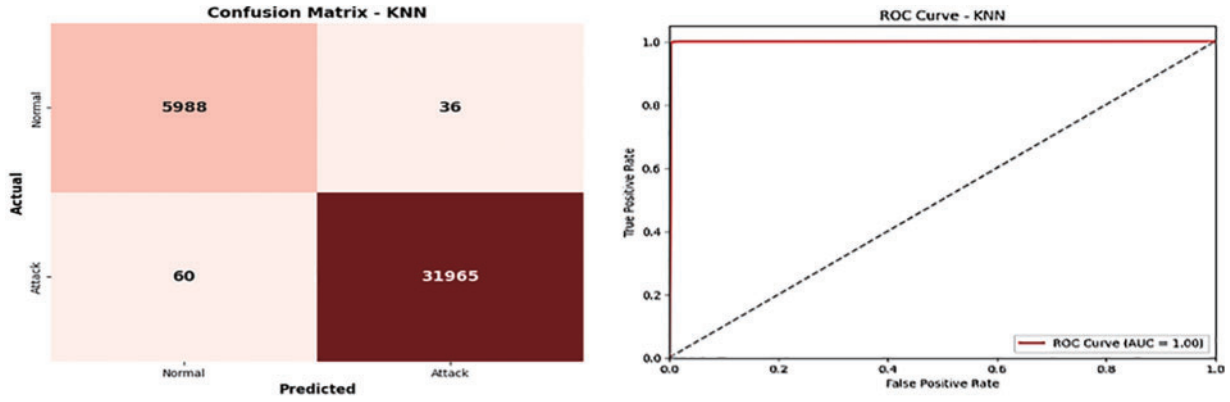

Figure 21: Confusion matrix for KNN model

e) SVM Classifier

In our assessment, we chose the Support Vector Machine (SVM) classifier, a robust supervised learning algorithm employed for both classification and regression tasks. The essence of the SVM algorithm lies in its ability to identify the optimal hyperplane that effectively separates classes in the feature space, maximizing the margin between them [131]. For our analysis, we concentrated on the linear support vector classifier (Linear SVC) variant of the SVM model. Linear SVC functions by determining the linear decision boundary that optimally separates classes, making it suitable for datasets with linear separability. The evaluation results shed light on the performance of the SVM Linear SVC Kernel model across various metrics: The model achieved an accuracy of 0.86, indicating the proportion of correctly classified instances. Sensitivity, also known as recall, reached a high value of 0.965, signifying the model's proficiency in accurately identifying positive instances. Precision, representing the proportion of true positive predictions among all positive predictions, stood at 0.88, demonstrating the reliability of positive predictions. The F1-score, a harmonic mean of precision and recall, reached 0.921, indicating a balance between precision and sensitivity. Additionally, recall matched sensitivity at 0.965, highlighting the model's ability to recall positive instances. While a detailed breakdown in Fig. 22 was provided, showcasing both the confusion matrix and the ROC curve, the confusion matrix offers a detailed view of the model's predictions across different classes. Conversely, the ROC curve illustrates its ability to balance sensitivity and specificity across various classification thresholds. In summary, the SVM Linear SVC Kernel model exhibited commendable performance in our evaluation, indicating its potential as a valuable tool for classification tasks, especially in scenarios characterized by linearly separable data.

f) Summary of Our Evaluation

Analyzing the evaluation results of our dataset using various machine learning techniques provides valuable insights into the effectiveness of different methods, as illustrated in Fig. 23. Let's explore a comparative analysis of these techniques:

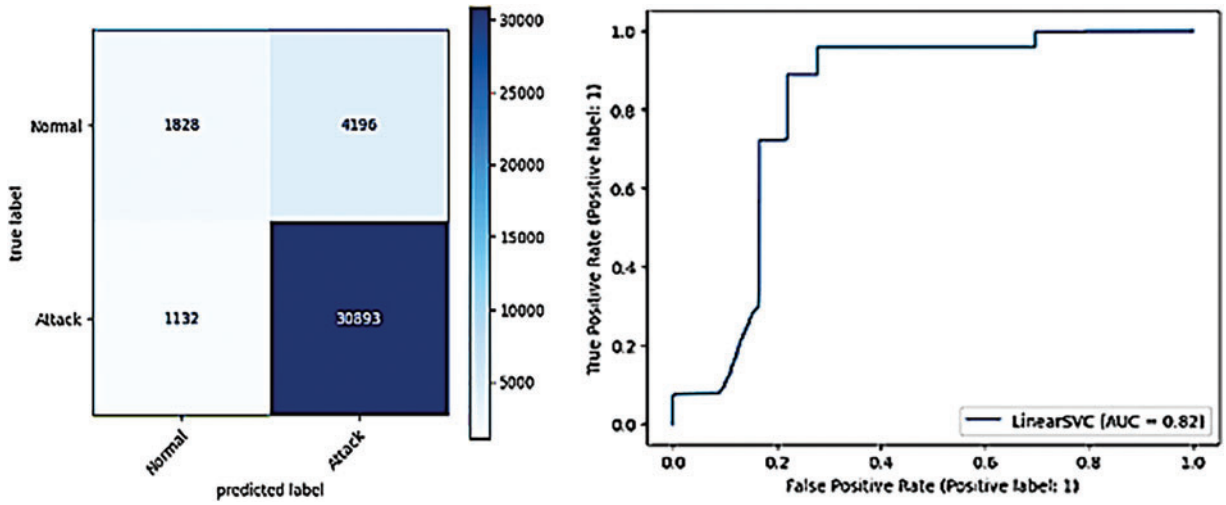

Figure 22: Confusion matrix for SVM classifier

Model	Accuracy	Sensitivity	Precision	F1 Score	Recall
Logistic Regression	0.894	0.996	0.891	0.941	0.996
Decision Tree Classifier	1.000	1.000	1.000	1.000	1.000
Random Forest Classifier	1.000	1.000	1.000	1.000	1.000
KNN-Model	0.997	0.998	0.999	0.999	0.998
SVM Classifier	0.860	0.965	0.880	0.921	0.965
Gradient Boosting Classifier	1.000	1.000	1.000	1.000	1.000
Extreme Gradient Boosting (XGBoost) Classifier	1.000	1.000	1.000	1.000	1.000
Light Gradient Boosting Machine (LGBM) Classifier	1.000	1.000	1.000	1.000	1.000
CatBoost Classifier	1.000	1.000	1.000	1.000	1.000
Naive Bayes Classifier	0.443	0.339	0.998	0.506	0.339
Linear Discriminant Analysis (LDA)	0.888	1.000	0.883	0.938	1.000
Quadratic Discriminant Analysis (QDA)	0.911	0.964	0.932	0.948	0.964

Figure 23: Evaluation results

Accuracy Assessment: The accuracy metric assesses the overall correctness of predictions across all classes. Notably, the Decision Tree Classifier, Random Forest Classifier, KNN-Model, Gradient Boosting Classifier, Extreme Gradient Boosting (XGBoost) Classifier, Light Gradient Boosting Machine (LGBM) Classifier, and CatBoost Classifier achieved perfect accuracy scores of 1.0, indicating flawless classification performance. However, methods such as Logistic Regression, SVM Classifier, Naive Bayes Classifier, Linear Discriminant Analysis (LDA), and Quadratic Discriminant Analysis (QDA) demonstrated slightly lower accuracy scores, suggesting varying degrees of predictive capability.

Sensitivity and Recall Analysis: Sensitivity (or recall) evaluates a model's ability to correctly identify positive instances. The Decision Tree Classifier, Random Forest Classifier, KNN-Model, Gradient Boosting Classifier, Extreme Gradient Boosting (XGBoost) Classifier, Light Gradient Boosting Machine (LGBM) Classifier, and CatBoost Classifier exhibited high sensitivity scores, indicating strong performance in accurately detecting positive cases. Conversely, other methods displayed differing sensitivity levels, highlighting disparities in their capacity to capture positive instances.

Precision Examination: Precision quantifies the ratio of true positive predictions among all positive predictions made by the model. Models with elevated precision scores, including the Decision Tree

Classifier, Random Forest Classifier, KNN-Model, Gradient Boosting Classifier, Extreme Gradient Boosting (XGBoost) Classifier, Light Gradient Boosting Machine (LGBM) Classifier, and CatBoost Classifier, showcased a minimal rate of false positive predictions. Conversely, Logistic Regression, SVM Classifier, Naive Bayes Classifier, Linear Discriminant Analysis (LDA), and Quadratic Discriminant Analysis (QDA) exhibited varying levels of precision.

F1-score Evaluation: The F1-score, which harmonizes precision and recall, provides insights into a model's overall performance. Remarkably, the Decision Tree Classifier, Random Forest Classifier, KNN-Model, Gradient Boosting Classifier, Extreme Gradient Boosting (XGBoost) Classifier, Light Gradient Boosting Machine (LGBM) Classifier, and CatBoost Classifier demonstrated high F1-scores, signifying a balanced trade-off between precision and recall. Conversely, Logistic Regression, SVM Classifier, Naive Bayes Classifier, Linear Discriminant Analysis (LDA), and Quadratic Discriminant Analysis (QDA) exhibited varying F1-scores, indicating diverse compromises between precision and recall.

In summary, our evaluation across different machine learning methodologies underscores their respective strengths and weaknesses in handling the dataset. Understanding these nuances is crucial for selecting the most suitable approach for specific tasks and optimizing overall model performance.

5.4.4 Multi Classification

In our multiclassification investigation, we transformed the "Attack Type" feature into 15 distinct values, ranging from 0 to 14, utilizing the LabelEncoder function. Each attack type, such as Backdoor, DDoS_HTTP, DDoS_ICMP, and others, received a unique encoded value. For example, Backdoor was encoded as 0, DDoS_HTTP as 1, and so forth, up to XSS, which was encoded as 14. This encoding enabled us to represent categorical data in a machine-learning-friendly format. The encoded values are visually depicted in Fig. 24 of our analysis, providing a clear mapping between attack types and their respective encoded representations. With this encoding scheme established, we proceeded to assess the performance of our models using various machine learning techniques for effective classification of the different attack types.

	Attack Type	Encoded Value
0	Backdoor	0
1	DDoS_HTTP	1
2	DDoS_ICMP	2
3	DDoS_TCP	3
4	DDoS_UDP	4
5	Fingerprinting	5
6	MITM	6
7	Normal	7
8	Password	8
9	Port_Scanning	9
10	Ransomware	10
11	SQL_injection	11
12	Uploading	12
13	Vulnerability_scanner	13
14	XSS	14

Figure 24: Encoded value for attack type

a) Logistic Regression

In our multiclassification analysis utilizing logistic regression, we attained an overall accuracy of approximately 47.16%. The classification report offers a thorough breakdown of the model's efficacy

across various attack types. Across different attack types, there are notable discrepancies in precision, recall, and F1-score values, indicating varying degrees of success in accurately identifying instances of each class. For instance, the model excelled in recognizing DDoS_UDP attacks, achieving nearly flawless precision, recall, and F1-score values of 1.00. Conversely, for attack types like Backdoor (Class 0), Password (Class 8), Port Scanning (Class 9), and others, the precision, recall, and F1-score values were comparatively lower, implying difficulties in precisely classifying instances of these attack types. On aggregate, the weighted average precision, recall, and F1-score stand at 0.40, 0.47, and 0.41, respectively as shown Fig. 25, providing a comprehensive assessment of the model's performance while considering class imbalances. Furthermore, the macro-average F1-score, at 0.37, represents the harmonic mean of precision and recall across all classes. Although logistic regression serves as a foundational model for multiclass classification, these findings underscore the necessity for further optimization or exploration of alternative algorithms to enhance classification accuracy, particularly for classes exhibiting lower precision, recall, and F1-scores.

Accuracy: 0.47157612552235273
Classification Report:

	precision	recall	f1-score	support
0	0.11	0.05	0.06	2430
1	0.48	0.31	0.38	2623
2	1.00	0.99	0.99	3247
3	0.34	0.60	0.43	2515
4	1.00	1.00	1.00	3645
5	0.84	0.67	0.74	219
6	0.06	0.97	0.12	91
7	0.34	0.89	0.50	6024
8	0.00	0.00	0.00	2540
9	0.00	0.00	0.00	2164
10	0.04	0.00	0.01	2385
11	0.00	0.00	0.00	2619
12	0.39	0.31	0.35	2512
13	0.73	0.73	0.73	2576
14	0.32	0.15	0.21	2459
accuracy			0.47	38049
macro avg	0.38	0.44	0.37	38049
weighted avg	0.40	0.47	0.41	38049

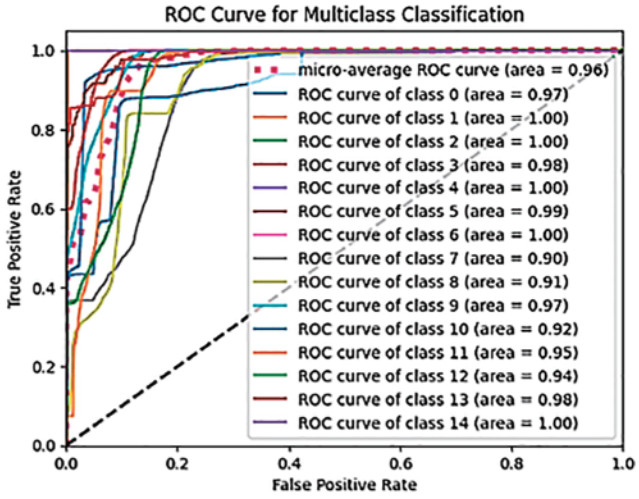

Figure 25: Evaluation model with logistic regression

b) Decision Tree Classifier

The multiclass classification conducted using the decision tree model delivered outstanding outcomes, boasting a remarkable accuracy of 99.99%, as illustrated in Fig. 26. This exceptionally high accuracy underscores the model's exceptional performance in accurately categorizing instances across all classes. Here's a detailed breakdown of the classification report:

Precision: Precision gauges the accuracy of positive predictions. Remarkably, the precision for all classes stands at 100%, indicating minimal false positive predictions made by the model.

Recall: Recall assesses the proportion of actual positive instances correctly classified by the model. Similar to precision, the recall for all classes is 100%, indicating the model's ability to capture nearly all positive instances.

F1-score: The F1-score represents the harmonic mean of precision and recall, offering a balanced assessment. Impressively, the F1-score for all classes is also 100%, indicating a perfect equilibrium between precision and recall.

Support: Support denotes the frequency of actual occurrences of each class in the test dataset. While support varies for each class, it generally maintains balance across classes. Overall, the Decision

Tree model demonstrated near-flawless performance across all evaluation metrics, affirming its efficacy in accurately addressing instances within the multiclass classification problem.

Accuracy: 0.9999737181003443
Classification Report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	2430
1	1.00	1.00	1.00	2623
2	1.00	1.00	1.00	3247
3	1.00	1.00	1.00	2515
4	1.00	1.00	1.00	3645
5	1.00	1.00	1.00	219
6	1.00	0.99	0.99	91
7	1.00	1.00	1.00	6024
8	1.00	1.00	1.00	2540
9	1.00	1.00	1.00	2164
10	1.00	1.00	1.00	2385
11	1.00	1.00	1.00	2619
12	1.00	1.00	1.00	2512
13	1.00	1.00	1.00	2576
14	1.00	1.00	1.00	2459
accuracy			1.00	38049
macro avg	1.00	1.00	1.00	38049
weighted avg	1.00	1.00	1.00	38049

Figure 26: Evaluation model with decision tree

c) Random Forest Classifier

In our multiclassification analysis employing the random forest classifier, we attained an exceptional accuracy level of approximately 99.99%. The classification report offers a deeper insight into the model's exemplary performance across diverse attack types. Across all attack types, precision, recall, and F1-score values uniformly register at 1.00, indicating flawless proficiency in accurately identifying instances of each class. This underscores the Random Forest classifier's adeptness in effectively distinguishing between various attack types with utmost precision and dependability.

Furthermore, the weighted average precision, recall, and F1-score also achieve a perfect score of 1.00, reflecting the model's stellar overall performance across all classes. Similarly, the macro-average F1-score and other metrics attain a score of 1.00, emphasizing the model's outstanding performance without any discernible disparities across different attack types. This remarkable performance is bolstered by the model's 100% accuracy rate, affirming the Random Forest classifier's precise prediction of the attack type for nearly all instances in the dataset. For comprehensive insights into the model's performance, including detailed results and the classification report, please refer to Fig. 27, facilitating thorough analysis and evaluation.

d) KNN-Model

In our multiclass classification endeavor employing the K-Nearest Neighbors (KNN) model, we attained an accuracy level of approximately 93.55%. The classification report furnishes a thorough breakdown of precision, recall, and F1-score for individual classes. Remarkably, the model demonstrated commendable performance across the majority of classes, showcasing high precision and recall values. Both macro and weighted averages reinforce the model's robust overall performance across all classes. These outcomes are meticulously presented in Fig. 28, providing detailed insights into the KNN model's efficacy for our multiclass classification undertaking.

Accuracy: 0.9996583353044758
Classification Report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	2430
1	1.00	1.00	1.00	2623
2	1.00	1.00	1.00	3247
3	1.00	1.00	1.00	2515
4	1.00	1.00	1.00	3645
5	1.00	1.00	1.00	219
6	1.00	0.99	0.99	91
7	1.00	1.00	1.00	6024
8	1.00	1.00	1.00	2540
9	1.00	1.00	1.00	2164
10	1.00	1.00	1.00	2385
11	1.00	1.00	1.00	2619
12	1.00	1.00	1.00	2512
13	1.00	1.00	1.00	2576
14	1.00	1.00	1.00	2459
accuracy			1.00	38049
macro avg	1.00	1.00	1.00	38049
weighted avg	1.00	1.00	1.00	38049

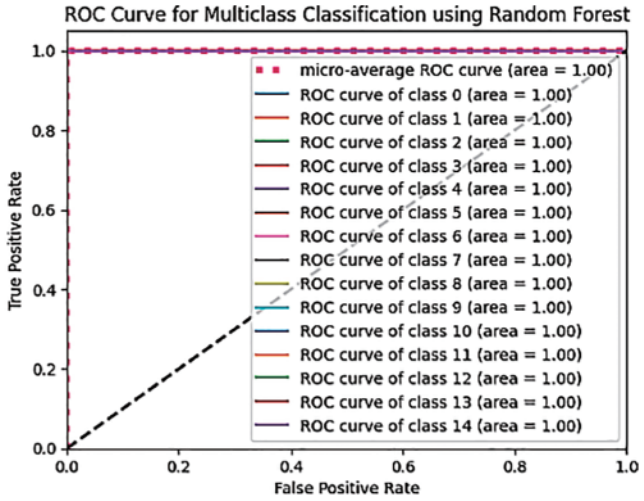

Figure 27: Evaluation model with random forest

Accuracy: 0.9355305001445504
Classification Report:

	precision	recall	f1-score	support
0	0.85	0.73	0.79	2430
1	1.00	1.00	1.00	2623
2	1.00	0.99	1.00	3247
3	0.74	0.78	0.76	2515
4	1.00	1.00	1.00	3645
5	0.88	0.99	0.93	219
6	1.00	0.99	0.99	91
7	0.99	0.99	0.99	6024
8	1.00	0.99	1.00	2540
9	0.73	0.69	0.71	2164
10	0.76	0.87	0.81	2385
11	0.97	1.00	0.99	2619
12	0.98	0.99	0.99	2512
13	0.99	0.95	0.97	2576
14	0.99	0.99	0.99	2459
accuracy			0.94	38049
macro avg	0.93	0.93	0.93	38049
weighted avg	0.94	0.94	0.94	38049

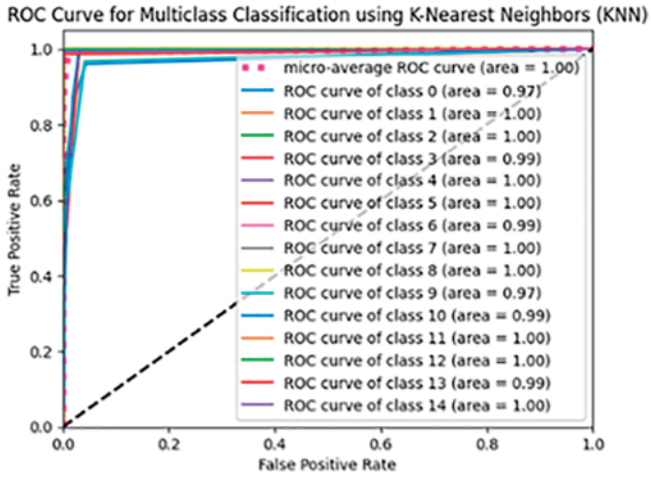

Figure 28: Evaluation model with KNN

e) SVM Classifier

The multiclass classification employing the Support Vector Machine (SVM) model yielded an accuracy of 37.04%. This accuracy suggests that the model's performance is relatively inadequate compared to other models. Here's an examination of the classification report:

Precision: For most classes, precision values are notably low or zero, indicating a considerable number of false positive predictions. Classes 2 and 4 exhibit relatively higher precision, implying that the model excelled in identifying these classes compared to others.

Recall: Across classes, recall values exhibit variation, with some achieving a recall of 100% (e.g., Class 4), while others register very low or zero recall. Class 7 attains a recall of 100%, indicating the model's effectiveness in capturing all instances of this class.

F1-score: The F1-score, representing the harmonic mean of precision and recall, remains low for the majority of classes. This suggests that the model encountered challenges in striking a balance between precision and recall for many classes.

Support: Support values demonstrate discrepancies across classes, highlighting the imbalance in the distribution of classes within the test dataset.

Overall, the SVM model's performance falls short, evident from its low accuracy and poor precision, recall, and F1-score across most classes. Further analysis, potentially involving model tuning, is warranted to enhance its performance in addressing this multiclass classification problem. These detailed findings are presented comprehensively in Fig. 29.

Accuracy: 0.37036452994822466
Classification Report:

	precision	recall	f1-score	support
0	0.00	0.00	0.00	2430
1	0.00	0.00	0.00	2623
2	0.97	0.96	0.96	3247
3	0.58	0.55	0.56	2515
4	1.00	0.99	0.99	3645
5	0.00	0.00	0.00	219
6	0.00	0.00	0.00	91
7	0.21	1.00	0.34	6024
8	0.00	0.00	0.00	2540
9	0.00	0.00	0.00	2164
10	0.00	0.00	0.00	2385
11	0.00	0.00	0.00	2619
12	0.00	0.00	0.00	2512
13	0.00	0.00	0.00	2576
14	0.00	0.00	0.00	2459
accuracy			0.37	38049
macro avg	0.18	0.23	0.19	38049
weighted avg	0.25	0.37	0.27	38049

Figure 29: Evaluation model with SVM

f) Discussion

The analysis of different machine learning models applied to the multiclassification task reveals substantial variations in performance. Notably, the random forest classifier yielded exceptional results with an accuracy of 99.97% and consistently high precision, recall, and F1-scores across all classes, indicating robust learning of underlying patterns. Conversely, Logistic Regression exhibited a lower accuracy of 47.16% and struggled with certain classes, suggesting difficulties in capturing complex relationships within the data. In contrast, the KNeighborsClassifier demonstrated strong performance with an accuracy of 93.55% and balanced precision, recall, and F1-scores across classes, reflecting effective pattern recognition. However, the SVM model underperformed, achieving an accuracy of 37.04% and displaying notable disparities in precision, recall, and F1-scores across classes, particularly in cases of imbalanced data distribution. Ultimately, both RandomForestClassifier and DecisionTreeClassifier stood out for their exceptional accuracy and balanced performance, highlighting their efficacy in tackling multiclassification tasks.

5.4.5 Comparison of Performance with Related Studies

The provided Table 1 offers a comprehensive comparison of performance accuracy across various models employed in different studies, including Decision Trees (DT), Random Forest (RF), Support

Vector Machine (SVM), K-Nearest Neighbors (KNN), Deep Neural Networks (DNN), Polynomial Bayes (Poly Br), Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM), and XGBoost. Here's a breakdown of the comparative analysis:

Table 1: Performance accuracy comparison for binary classification with related articles

Article	DT	RF	SVM	KNN	DNN	Poly Br	CNN-LSTM	Xgboost
[132]	99.98	99.99	99.99	99.99	99.99	–	–	–
[133]	–	–	–	–	–	97.27	–	–
[134]	–	–	–	–	–	–	97.85	–
[135]	–	–	–	–	–	–	–	100
This study	100	100	86	99.70	–	–	–	–

Both our study and the referenced article [132] achieved perfect accuracy scores of 100% for both DT and RF models. This indicates exceptional performance in accurately classifying instances within IIoT networks. While the referenced article attained a high accuracy of 99.99% for SVM, our study reported a lower accuracy of 86%. This disparity suggests potential differences in preprocessing techniques or model configurations between the two studies. The referenced article achieved a near-perfect accuracy of 99.99% for KNN, whereas our study reported a slightly lower accuracy of 99.70%. Nonetheless, both studies demonstrate robust performance in KNN classification. DNN performance was not reported in our study, indicating a potential area for future research. However, the referenced article achieved an impressive accuracy of 99.99% with DNN, highlighting its efficacy in detecting malicious activities within IIoT networks. Additional studies [133]–[135] also presented their results, showcasing accuracies ranging from 97.27% to 100% across different models such as Polynomial Bayes, CNN-LSTM, and XGBoost. Overall, our comparative analysis underscores the notable enhancement achieved through our proposed study, particularly in terms of Decision Trees and Random Forest models. However, disparities in SVM performance warrant further investigation into preprocessing methodologies and model configurations. Additionally, exploring the potential of Deep Neural Networks could further enhance detection capabilities in IIoT networks.

6 Conclusion

In Conclusion, our exploration of smart city applications, architecture, and characteristics highlights the transformative potential of advanced technologies in urban development. From smart mobility to healthcare, these applications aim to enhance efficiency, sustainability, and residents' quality of life. However, we recognize that the true novelty of smart cities lies not only in the apps themselves but also in the strategic utilization of supporting technologies such as IoT, cloud computing, and sensor networks.

Despite the promises of smart cities, significant security challenges loom large. Cybersecurity risks, data privacy concerns, and infrastructure resilience are formidable obstacles that we must address to realize the full potential of smart city objectives. We firmly believe that innovative security methods, from proactive threat detection to resilient infrastructure design, are imperative to safeguard the digital resilience of smart cities and ensure their continued success in an increasingly complex urban landscape.

Our proposed multifaceted strategy for mitigating cybersecurity challenges in smart cities emphasizes proactive and data-driven approaches to identifying and neutralizing potential threats. Leveraging advanced analytics and machine learning algorithms enables us to detect hidden patterns and indicators of compromise in real-time, fostering a culture of collective vigilance and resilience against emerging cyber threats.

Furthermore, our evaluation of different machine learning models for intrusion detection provides valuable insights into their performance across various tasks. Notably, models like RandomForestClassifier and DecisionTreeClassifier demonstrate exceptional accuracy and balanced performance, highlighting their efficacy in tackling multiclassification tasks. We understand that understanding these nuances is crucial for selecting the most suitable approach for specific tasks and optimizing overall model performance.

In this article, we have extensively utilized machine learning techniques to address the challenges associated with detecting malicious activities within IIoT networks. However, for our future endeavors, we aim to delve deeper into the realm of deep learning methods. Building upon the foundation laid by this research, our future work will focus on harnessing the power of deep learning algorithms to further enhance the detection capabilities in IIoT environments. By leveraging the inherent strengths of deep learning, such as its ability to automatically learn intricate patterns and representations from data, we anticipate achieving even more robust and accurate detection models. Through this transition to deep learning methodologies, we aim to push the boundaries of detection performance and contribute significantly to the advancement of security solutions for IIoT networks.

In essence, safeguarding smart cities requires a comprehensive approach that combines technical solutions with policy enhancements, governance frameworks, and educational efforts. By continuously adapting to emerging threats and fostering collaboration among stakeholders, we can fortify smart cities' cyber defenses and ensure the integrity, confidentiality, and availability of critical infrastructure and services for the benefit of all residents and stakeholders.

Future Developments and Improvements

Looking ahead, several key developments and improvements are anticipated in the field of smart city security and privacy. The integration of advanced deep learning techniques will play a pivotal role in enhancing threat detection accuracy and efficiency. There will also be a significant focus on developing more sophisticated data encryption and anonymization methods to ensure robust data privacy. Additionally, the implementation of blockchain technology for secure and transparent data transactions within smart cities is expected to gain traction. Innovations in proactive threat detection mechanisms and resilient infrastructure design will further bolster the security of smart cities. Collaborative efforts among policymakers, technology developers, and urban planners will be essential to create governance frameworks that can swiftly adapt to emerging cyber threats, ensuring the long-term security and privacy of smart city environments.

Acknowledgement: The authors would like to thank Sup'Com (Higher School of Communication of Tunis) and its affiliated organizations for their support and assistance during this research.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Mehdi Houichi, Faouzi Jaidi; data collection: Faouzi Jaidi; analysis and interpretation of results: Mehdi Houichi, Faouzi Jaidi, Adel Bouhoula; draft manuscript preparation: Faouzi Jaidi, Adel Bouhoula. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author, Mehdi Houichi, upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. Ismagilova, L. Hughes, Y. K. Dwivedi, and K. R. Raman, "Smart cities: Advances in research—An information systems perspective," *Int. J. Inf. Manag.*, vol. 47, pp. 88–100, 2019. doi: 10.1016/j.ijinfomgt.2019.01.004.

[2] A. Majid, "Security and privacy concerns over IoT devices attacks in smart cities (2022)," *J. Comput. Commun.*, vol. 11, no. 1, pp. 26–42, 2023.

[3] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Inf. Syst. Front.*, vol. 23, pp. 1–22, 2020. doi: 10.1007/s10796-020-10044-1.

[4] S. Praharaj, "A comprehensive analysis of the challenges and opportunities of the 100 smart cities mission in India," 2019. Accessed: Jun. 18, 2024. [Online]. Available: https://unsworks.unsw.edu.au/entities/publication/b83644bb-e925-4cfa-8c54-f85deabad9fd/full

[5] B. F. Barrett, A. DeWit, and M. Yarime, "Japanese smart cities and communities: Integrating technological and institutional innovation for Society 5.0," in *Smart Cities for Technological and Social Innovation*. Hoboken, New Jersey, NJ, USA: Academic Press, 2021, pp. 73–94. doi: 10.1016/B978-0-12-818886-6.00005-8.

[6] A. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert. Syst.*, vol. 39, no. 5, 2022, Art. no. e12753. doi: 10.1111/exsy.12753.

[7] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, 2022, Art. no. e3677. doi: 10.1002/ett.3677.

[8] R. Creemers, "China's conception of cyber sovereignty," in *Governing Cyberspace: Behavior, Power, and Diplomacy*, A. B. Wright and J. M. Brown, eds. Oxford: Oxford University Press, 2020, pp. 107–145.

[9] T. Braun, B. C. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustain. Cities Soc.*, vol. 39, no. 4, pp. 499–507, 2018. doi: 10.1016/j.scs.2018.02.039.

[10] A. Finogeev, A. Finogeev, L. Fionova, A. Lyapin, and K. A. Lychagin, "Intelligent monitoring system for smart road environment," *J. Ind. Inf. Integr.*, vol. 15, no. 8, pp. 15–20, 2019. doi: 10.1016/j.jii.2019.05.003.

[11] N. S. Safa, F. Mitchell, C. Maple, M. A. Azad, and M. Dabbagh, "Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities," *Trans. Emerg. Telecomm. Technol.*, vol. 33, no. 10, 2022, Art. no. e4173. doi: 10.1002/ett.4173.

[12] J. C. F. De Guimarães, E. A. Severo, L. A. F. Júnior, W. P. L. B. Da Costa, and F. T. Salmoria, "Governance and quality of life in smart cities: Towards sustainable development goals," *J. Clean. Prod.*, vol. 253, no. 1, 2020, Art. no. 119926. doi: 10.1016/j.jclepro.2019.119926.

[13] S. K. Rathor and D. Saxena, "Energy management system for smart grid: An overview and key issues," *Int. J. Energy Res.*, vol. 44, no. 6, pp. 4067–4109, 2020. doi: 10.1002/er.4883.

[14] Y. M. Guo, Z. L. Huang, J. Guo, H. Li, X. R. Guo and M. J. Nkeli, "Bibliometric analysis on smart cities research," *Sustainability*, vol. 11, no. 13, 2019, Art. no. 3606. doi: 10.3390/su11133606.

[15] M. A. S. Kamal, T. Hayakawa, and J. I. Imura, "Development and evaluation of an adaptive traffic signal control scheme under a mixed-automated traffic scenario," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 2, pp. 590–602, 2019. doi: 10.1109/TITS.2019.2896943.

[16] Z. Mahrez, E. Sabir, E. Badidi, W. Saad, and M. Sadik, "Smart urban mobility: When mobility systems meet smart data," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6222–6239, 2021. doi: 10.1109/TITS.2021.3084907.

[17] K. Lee and I. N. Sener, "Strava Metro data for bicycle monitoring: A literature review," *Transp. Rev.*, vol. 41, no. 1, pp. 27–47, 2021. doi: 10.1080/01441647.2020.1798558.

[18] A. Ş. Chenic *et al.*, "Logical analysis on the strategy for a sustainable transition of the world to green energy—2050. Smart cities and villages coupled to renewable energy sources with low carbon footprint," *Sustainability*, vol. 14, no. 14, 2022, Art. no. 8622. doi: 10.3390/su14148622.

[19] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid and M. Zuair, "A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid," *IEEE Access*, vol. 8, pp. 47047–47062, 2020. doi: 10.1109/ACCESS.2020.2979051.

[20] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng and P. Singh, "Secure and energy-efficient smart building architecture with emerging technology IoT," *Comput. Commun.*, vol. 176, no. 3, pp. 207–217, 2021. doi: 10.1016/j.comcom.2021.06.003.

[21] C. Stolojescu-Crisan, C. Crisan, and B. P. Butunoi, "An IoT-based smart home automation system," *Sensors*, vol. 21, no. 11, 2021, Art. no. 3784. doi: 10.3390/s21113784.

[22] A. Kakar, S. Agrawal, and G. Sumathi, "Smart home: A new way to life," in *2021 Innov. Power Adv. Comput. Technol. (i-PACT)*, IEEE, Nov. 2021, pp. 1–6.

[23] E. Weber *et al.*, "Detecting natural disasters, damage, and incidents in the wild," in *Comput. Vis.—ECCV 2020: 16th Eur. Conf.*, Glasgow, UK, Springer International Publishing, 2020, pp. 331–350.

[24] Y. A. Fatimah, K. Govindan, R. Murniningsih, and A. Setiawan, "Industry 4.0 based sustainable circular economy approach for smart waste management system to achieve sustainable development goals: A case study of Indonesia," *J. Clean. Prod.*, vol. 269, no. 3, 2020, Art. no. 122263. doi: 10.1016/j.jclepro.2020.122263.

[25] S. Viswanathan, S. Momand, M. Fruten, and A. Alcantar, "A model for the assessment of energy-efficient smart street lighting—A case study," *Energy Effic.*, vol. 14, no. 6, 2021, Art. no. 52. doi: 10.1007/s12053-021-09957-w.

[26] M. Ncamphalala, "The role of ICT to promote smart governance in local governments," Doctoral dissertation, Univ. of Johannesburg, South Africa, 2019.

[27] N. Goodman, A. Zwick, Z. Spicer, and N. Carlsen, "Public engagement in smart city development: Lessons from communities in Canada's smart city challenge," *Canadian Geographer/Le Géographe Canadien*, vol. 64, no. 3, pp. 416–432, 2020. doi: 10.1111/cag.12607.

[28] R. Wolniak, B. Gajdzik, M. Grebski, R. Danel, and W. W. Grebski, "Business models used in smart cities—theoretical approach with examples of smart cities," *Smart Cities*, vol. 7, no. 4, pp. 1626–1669, 2024. doi: 10.3390/smartcities7040065.

[29] L. Syed, S. Jabeen, S. Manimala, and A. Alsaeedi, "Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques," *Future Gener. Comput. Syst.*, vol. 101, no. 3, pp. 136–151, 2019. doi: 10.1016/j.future.2019.06.004.

[30] K. Kuru and D. Ansell, "TCitySmartF: A comprehensive systematic framework for transforming cities into smart cities," *IEEE Access*, vol. 8, pp. 18615–18644, 2020. doi: 10.1109/ACCESS.2020.2967777.

[31] Z. Yousif, I. Hussain, S. Djahel, and Y. Hadjadj-Aoul, "A novel energy-efficient clustering algorithm for more sustainable wireless sensor networks enabled smart cities applications," *J. Sens. Actuator Netw.*, vol. 10, no. 3, p. 50, 2021. doi: 10.3390/jsan10030050.

[32] S. M. Antony, S. Indu, and R. Pandey, "An efficient solar energy harvesting system for wireless sensor network nodes," *J. Inf. Optim. Sci.*, vol. 41, no. 1, pp. 39–50, 2020. doi: 10.1080/02522667.2020.1714182.

[33] L. Guevara and F. Auat Cheein, "The role of 5G technologies: Challenges in smart cities and intelligent transportation systems," *Sustainability*, vol. 12, no. 16, 2020, Art. no. 6469. doi: 10.3390/su12166469.

[34] E. Alyavina, A. Nikitas, and E. T. Njoya, "Mobility as a service and sustainable travel behaviour: A thematic analysis study," *Transp. Res. F: Traffic Psychol. Behav.*, vol. 73, no. 2, pp. 362–381, 2020. doi: 10.1016/j.trf.2020.07.004.

[35] W. I. R. A. J. Gunasinghe, "Cloud based secure element implementation for android host card emulation," Accessed: Apr. 5, 2024. [Online]. Available: https://dl.ucsc.cmb.ac.lk/jspui/handle/123456789/4261

[36] P. Muzikant and J. Hajný, "Integrating smart card authentication to web applications," in *2022 14th Int. Congress Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Valencia, Spain, IEEE, Oct. 2022, pp. 90–95.

[37] N. P. Kozievitch *et al.*, "Assessment of open data portals: A Brazilian case study," in *IEEE Int. Smart Cities Conf. (ISC2)*, Paphos, Cyprus, IEEE, Sep. 2022, pp. 1–7.

[38] A. Hilmani, A. Maizate, and L. Hassouni, "Automated real-time intelligent traffic control system for smart cities using wireless sensor networks," *Wirel. Commun. Mob. Comput.*, vol. 2020, no. 1, pp. 1–28, 2020. doi: 10.1155/2020/8841893.

[39] S. E. Bibri, "The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability," *Sustain. Cities Soc.*, vol. 38, no. 1, pp. 230–253, 2018. doi: 10.1016/j.scs.2017.12.034.

[40] H. Raad, *Fundamentals of IoT and Wearable Technology Design*, 1st ed. Hoboken, New Jersey, USA: John Wiley & Sons, 2020.

[41] N. Y. Philip, J. J. Rodrigues, H. Wang, S. J. Fong, and J. Chen, "Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 300–310, 2021. doi: 10.1109/JSAC.2020.3042421.

[42] M. Ryalat, H. ElMoaqet, and M. AlFaouri, "Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0," *Appl. Sci.*, vol. 13, no. 4, 2023, Art. no. 2156. doi: 10.3390/app13042156.

[43] R. Porteiro and S. Nesmachnow, "Detecting air conditioning usage in households using unsupervised machine learning on smart meter data," in *Smart Cities: 5th Ibero-American Congress, ICSC-CITIES 2022,* Cuenca, Ecuador, Cham: Springer Nature Switzerland, Mar. 2023, pp. 233–247.

[44] A. Gohari, A. B. Ahmad, R. B. A. Rahim, A. S. M. Supa'at, S. Abd Razak and M. S. M. Gismalla, "Involvement of surveillance drones in smart cities: A systematic review," *IEEE Access*, vol. 10, pp. 56611–56628, 2022. doi: 10.1109/ACCESS.2022.3177904.

[45] M. Liu, J. Wu, C. Zhu, and K. Hu, "A study on public adoption of robo-taxis in China," *J. Adv. Transp.*, vol. 2020, no. 4, pp. 1–8, 2020. doi: 10.1155/2020/8846955.

[46] G. Sun, R. Zhou, J. Sun, H. Yu, and A. V. Vasilakos, "Energy-efficient provisioning for service function chains to support delay-sensitive applications in network function virtualization," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6116–6131, 2020. doi: 10.1109/JIOT.2020.2970995.

[47] C. Zhang, "Design and application of fog computing and Internet of Things service platform for smart city," *Future Gener. Comput. Syst.*, vol. 112, no. 6, pp. 630–640, 2020. doi: 10.1016/j.future.2020.06.016.

[48] G. P. Hancke and G. P. Hancke Jr, "The role of advanced sensing in smart cities," *Sensors*, vol. 13, no. 1, pp. 393–425, 2013. doi: 10.3390/s130100393.

[49] M. Houichi, F. Jaidi, and A. Bouhoula, "A systematic approach for IoT cyber-attacks detection in smart cities using machine learning techniques," in *Int. Conf. Adv. Inf. Netw. Appl.*, Toronto, ON, Canada, Cham: Springer International Publishing, Apr. 2021, pp. 215–228.

[50] S. D. Sandhya Devi , V. R. Vijaykumar, and P. Sivakumar, "Edge architecture integration of technologies," in *Cases on Edge Computing and Analytics*. Hershey, PA, USA: IGI Global, 2021, pp. 1–30.

[51] S. P. Ramu *et al.*, "Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions," *Sustain. Cities Soc.*, vol. 79, no. 1, 2022, Art. no. 103663. doi: 10.1016/j.scs.2021.103663.

[52] A. Hazra, P. Rana, M. Adhikari, and T. Amgoth, "Fog computing for next-generation internet of things: Fundamental, state-of-the-art and research challenges," *Comput. Sci. Rev.*, vol. 48, no. 5, 2023, Art. no. 100549. doi: 10.1016/j.cosrev.2023.100549.

[53] H. S. M. Lim and A. Taeihagh, "Algorithmic decision-making in AVs: Understanding ethical and technical concerns for smart cities," *Sustainability*, vol. 11, no. 20, 2019, Art. no. 5791. doi: 10.3390/su11205791.

[54] M. H. Amini, H. Arasteh, and P. Siano, "Sustainable smart cities through the lens of complex interdependent infrastructures: Panorama and state-of-the-art," in *Sustainable Interdependent Networks II: From Smart Power Grids to Intelligent Transportation Networks*, Cham, Switzerland, 2019, pp. 45–68.

[55] G. Perboli, A. De Marco, F. Perfetti, and M. Marone, "A new taxonomy of smart city projects," *Transp. Res. Procedia*, vol. 3, pp. 470–478, 2014. doi: 10.1016/j.trpro.2014.10.028.

[56] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente, "On the difficulty of software-based attestation of embedded devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Chicago, MI, USA, Nov. 2009, pp. 400–409.

[57] M. Lom, O. Pribyl, and M. Svitek, "Industry 4.0 as a part of smart cities," in *2016 Smart Cities Symp. Prague (SCSP)*, Prague Czech Republic, IEEE, May 2016, pp. 1–6.

[58] W. Van Winden and D. Van den Buuse, "Smart city pilot projects: Exploring the dimensions and conditions of scaling up," *J. Urban Technol.*, vol. 24, no. 4, pp. 51–72, 2017. doi: 10.1080/10630732.2017.1348884.

[59] N. Taylor Buck and A. While, "Competitive urbanism and the limits to smart city innovation: The UK Future Cities initiative," *Urban Stud.*, vol. 54, no. 2, pp. 501–519, 2017. doi: 10.1177/0042098015597162.

[60] S. Clever, T. Crago, A. Polka, J. Al-Jaroodi, and N. Mohamed, "Ethical analyses of smart city applications," *Urban Sci.*, vol. 2, no. 4, 2018, Art. no. 96. doi: 10.3390/urbansci2040096.

[61] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Veh. Commun.*, vol. 23, 2020, Art. no. 100214. doi: 10.1016/j.vehcom.2019.100214.

[62] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," *IEEE Trans. Syst., Man, Cybernetics, C (Appl. Rev.)*, vol. 42, no. 6, pp. 1190–1203, 2012. doi: 10.1109/TSMCC.2012.2189204.

[63] G. Kambourakis, C. Kolias, and A. Stavrou, "The mirai botnet and the iot zombie armies," in *MILCOM 2017—2017 IEEE Military Commun. Conf. (MILCOM)*, Baltimore, USA, IEEE, Oct. 2017, pp. 267–272.

[64] J. Boeglin, "The costs of self-driving cars: Reconciling freedom and privacy with tort liability in autonomous vehicle regulation," *Yale JL Tech.*, vol. 17, p. 171, 2015.

[65] B. R. Payne, "Car hacking: Accessing and exploiting the can bus protocol," *J. Cybersecur. Edu., Res. Practice*, vol. 2019, no. 1, 2019, Art. no. 5. doi: 10.62915/2472-2707.1045.

[66] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Commun. Surveys Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021. doi: 10.1109/COMST.2021.3064507.

[67] A. Piplai, S. S. L. Chukkapalli, and A. Joshi, "NAttack! Adversarial Attacks to bypass a GAN based classifier trained to detect Network intrusion," in *2020 IEEE 6th Int. Conf. Big Data Security Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput.,(HPSC) and IEEE Int. Conf. Intell. Data Security (IDS)*, Baltimore, MD, USA, IEEE, May 2020, pp. 49–54.

[68] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries:technologies, applications, and challenges," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 8, pp. 10517–10553, 2023. doi: 10.1007/s12652-022-03707-1.

[69] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, 2017. doi: 10.1109/MCOM.2017.1600267CM.

[70] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, 2018. doi: 10.1016/j.jmsy.2018.04.007.

[71] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, 2019, Art. no. 326. doi: 10.3390/s19020326.

[72] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, 2022, Art. no. 100547. doi: 10.1016/j.ijcip.2022.100547.

[73] S. Saini, A. Chauhan, G. Thakur, and L. Sapra, "Challenges and opportunities in secure smart cities for enhancing the security and privacy," in *Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities*, Cham, Switzerland, 2023, pp. 1–27.

[74] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, 2014. doi: 10.1109/ACCESS.2014.2362522.

[75] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *J. Syst. Archit.*, vol. 105, no. 1, 2020, Art. no. 101701. doi: 10.1016/j.sysarc.2019.101701.

[76] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019. doi: 10.1186/s42400-019-0038-7.

[77] K. Vaigandla, N. Azmi, and R. Karne, "Investigation on Intrusion Detection Systems (IDSs) in IoT," *Int. J.Emerg. Trends Eng, Res.*, vol. 10, no. 3, pp. 281–286, 2022.

[78] G. Abdiyeva-Aliyeva and M. Hematyar, "Statistic Approached dynamically detecting security threats and updating a signature-based intrusion detection system's database in NGN," *J. Adv. Inf. Technol.*, vol. 13, no. 5, 2022. doi: 10.12720/jait.13.5.524-529.

[79] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu and L. Zhang, "A comprehensive survey on DNS tunnel detection," *Comput. Netw.*, vol. 197, no. 3, 2021, Art. no. 108322. doi: 10.1016/j.comnet.2021.108322.

[80] J. V. V. Silva, N. R. de Oliveira, D. S. Medeiros, M. A. Lopez, and D. M. Mattos, "A statistical analysis of intrinsic bias of network security datasets for training machine learning mechanisms," *Annals Telecommun.*, vol. 77, no. 7–8, pp. 555–571, 2022. doi: 10.1007/s12243-021-00904-5.

[81] J. A. Herrera Silva, L. I. Barona López, Á.L. Valdivieso Caraguay, and M. Hernández-Álvarez, "A survey on situational awareness of ransomware attacks—detection and prevention parameters," *Remote Sens.*, vol. 11, no. 10, 2019, Art. no. 1168. doi: 10.3390/rs11101168.

[82] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig and S. Sanguanpong, "Search: A collaborative and intelligent nids architecture for sdn-based cloud IoT networks," *IEEE Access*, vol. 7, pp. 107678–107694, 2019. doi: 10.1109/ACCESS.2019.2932438.

[83] A. R. Javed, S. Ur Rehman, M. U. Khan, M. Alazab, and T. Reddy, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, 2021. doi: 10.1109/TNSE.2021.3059881.

[84] A. Heidari and M. A. Jabraeil Jamali, *Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions*. Cham, Switzerland: Cluster Computing, 2022, pp. 1–28.

[85] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018. doi: 10.1109/ACCESS.2018.2853985.

[86] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustain. Cities Soc.*, vol. 61, no. 2, 2020, Art. no. 102301. doi: 10.1016/j.scs.2020.102301.

[87] D. Popescul and L. D. Genete, "Data security in smart cities: Challenges and solutions," *Informatica Economică*, vol. 20, no. 1, pp. 29–38, 2016. doi: 10.12948/issn14531305/20.1.2016.03.

[88] M. Rahouti, K. Xiong, and Y. Xin, "Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends," *IEEE Access*, vol. 9, pp. 12083–12113, 2020. doi: 10.1109/ACCESS.2020.3047996.

[89] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wirel. Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014. doi: 10.1007/s11276-014-0761-7.

[90] L. Xia, D. T. Semirumi, and R. Rezaei, "A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy," *Sustain. Cities Soc.*, vol. 98, no. 2, 2023, Art. no. 104771. doi: 10.1016/j.scs.2023.104771.

[91] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021. doi: 10.1109/ACCESS.2021.3052867.

[92] S. Gupta *et al*., "Secure and lightweight authentication protocol for privacy preserving communications in smart city applications," *Sustainability*, vol. 15, no. 6, 2023, Art. no. 5346. doi: 10.3390/su15065346.
[93] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight privacy-preserving scheme using homomorphic encryption in industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14542–14550, 2021. doi: 10.1109/JIOT.2021.3066427.
[94] A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba and O. Said, "Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things," *J. Ambient Intell. Humaniz. Comput.*, pp. 1–11, 2022. doi: 10.1007/s12652-021-03459-4.
[95] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, 2018, Art. no. 2575. doi: 10.3390/s18082575.
[96] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," *J. Netw. Comput. Appl.*, vol. 181, no. 5, 2021, Art. no. 103050. doi: 10.1016/j.jnca.2021.103050.
[97] S. Gong, E. Tcydenova, J. Jo, Y. Lee, and J. H. Park, "Blockchain-based secure device management framework for an internet of things network in a smart city," *Sustainability*, vol. 11, no. 14, 2019, Art. no. 3889. doi: 10.3390/su11143889.
[98] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Inf. Process. Manag.*, vol. 58, no. 3, 2021, Art. no. 102482. doi: 10.1016/j.ipm.2020.102482.
[99] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics," *J. Netw. Comput. Appl.*, vol. 168, no. 1, 2020, Art. no. 102761. doi: 10.1016/j.jnca.2020.102761.
[100] J. Sooriyaarachchi, S. Seneviratne, K. Thilakarathna, and A. Y. Zomaya, "MusicID: A brainwave-based user authentication system for internet of things," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8304–8313, 2020. doi: 10.1109/JIOT.2020.3044726.
[101] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3599–3609, 2017. doi: 10.1109/TII.2017.2773666.
[102] K. Almulla, "Cyber-attack detection in network traffic using machine learning," M.S. thesis, Grad. Prog. Res. Rochester Inst. Technol., Dubai, 2022. Accessed: Apr. 19, 2024. [Online]. Available: https://repository.rit.edu/theses/11320
[103] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "IoT in smart cities: A survey of technologies, practices and challenges," *Smart Cities*, vol. 4, no. 2, pp. 429–475, 2021. doi: 10.3390/smartcities4020024.
[104] M. A. Rahman, A. T. Asyhari, O. W. Wen, H. Ajra, Y. Ahmed and F. Anwar, "Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 31381–31399, 2021. doi: 10.1007/s11042-021-10567-y.
[105] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. Ehatisham-ul-Haq, and M. A. Azam, "Identifying smartphone users based on how they interact with their phones," *Hum. Centric Comput. Inf. Sci.*, vol. 10, no. 1, 2020, Art. no. 7. doi: 10.1186/s13673-020-0212-7.
[106] M. Zhu, A. H. Anwar, Z. Wan, J. H. Cho, C. Kamhoua and M. P. Singh, "Game-theoretic and machine learning-based approaches for defensive deception: A survey," 2021, *arXiv:2101.10121*.
[107] A. Rawal, D. Rawat, and B. M. Sadler, "Recent advances in adversarial machine learning: status, challenges and perspectives," *Artif. Intell. Mach. Learn. Multi-Domain Operat. Appl. III*, vol. 11746, pp. 701–712, 2021.
[108] F. Anwar, B. U. I. Khan, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A comprehensive insight into game theory in relevance to cyber security," *Indones. J. Electr. Eng. Inform.*, vol. 8, no. 1, pp. 189–203, 2020.
[109] M. Zhu, A. H. Anwar, Z. Wan, J. H. Cho, C. A. Kamhoua and M. P. Singh, "A survey of defensive deception: Approaches using game theory and machine learning," *IEEE Commun. Surveys Tutorials*, vol. 23, no. 4, pp. 2460–2493, 2021. doi: 10.1109/COMST.2021.3102874.

[110] K. S. Gill, A. Sharma, and S. Saxena, "A systematic review on game-theoretic models and different types of security requirements in cloud environment: Challenges and opportunities," *Arch. Comput. Methods Eng.*, pp. 1–34, 2024. doi: 10.1007/s11831-024-10095-6.

[111] Z. Li, "Detecting malware with securedeep accelerator via processor side-channel fingerprinting for Internet of Things," Ph.D. dissertation, Comput. Sci., Old Dominion Univ., 2023. doi: 10.25777/jhs5-db32.

[112] L. Shi, X. Wang, and H. Hou, "Research on optimization of array honeypot defense strategies based on evolutionary game theory," *Mathematics*, vol. 9, no. 8, 2021, Art. no. 805. doi: 10.3390/math9080805.

[113] Y. W. Kassa, J. I. James, and E. G. Belay, "Cybercrime intention recognition: A systematic literature review," *Information*, vol. 15, no. 5, 2024, Art. no. 263. doi: 10.3390/info15050263.

[114] M. Tao, K. Ota, and M. Dong, "Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes," *Future Gener. Comput. Syst.*, vol. 76, no. 6, pp. 528–539, 2017. doi: 10.1016/j.future.2016.11.012.

[115] S. K. Shahzad, D. Ahmed, M. R. Naqvi, M. T. Mushtaq, M. W. Iqbal and F. Munir, "Ontology driven smart health service integration," *Comput. Methods Programs Biomed.*, vol. 207, no. 12, 2021, Art. no. 106146. doi: 10.1016/j.cmpb.2021.106146.

[116] E. Onu, "Personalized Privacy Preservation in IoT," Doctoral dissertation, Univ. of Calgary, Alberta, Canada, 2022.

[117] N. Iqbal, M. A. Khan, A. Rizwan, and D. H. Kim, "Semantic situation reporting mechanism based on 4W'H ontology modeling in battlefield," *J. Intell. Pervasive Soft Comput.*, vol. 1, no. 1, pp. 25–31, 2022.

[118] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017. doi: 10.1016/j.telpol.2017.09.003.

[119] A. Christofi, "Smart cities and the data protection framework in context," 2021. Accessed: Apr. 25, 2024. [Online]. Available: https://scholar.google.com/scholar?hl=zh-CN&as_sdt=0%2C5&q=%09Christofi%2C+A.+%282021%29.+Smart+cities+and+the+data+protection+framework+in+context.&btnG=

[120] A. Degbelo, C. Granell, S. Trilles, D. Bhattacharya, S. Casteleyn and C. Kray, "Opening up smart cities: Citizen-centric challenges and opportunities from GIScience," *ISPRS Int. J. Geo Inf.*, vol. 5, no. 2, p. 16, 2016. doi: 10.3390/ijgi5020016.

[121] S. Barth and M. D. De Jong, "The privacy paradox-Investigating discrepancies between expressed privacy concerns and actual online behavior-A systematic literature review," *Telematics Inform.*, vol. 34, no. 7, pp. 1038–1058, 2017. doi: 10.1016/j.tele.2017.04.013.

[122] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach," *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 107–127, 2023. doi: 10.1007/s11036-022-02042-1.

[123] A. Sahbi, F. Jaidi, and A. Bouhoula, "Machine learning algorithms for enhancing intrusion detection within SDN/NFV," in *2023 Int. Wirel. Commun. Mobile Comput. (IWCMC)*, Marrakech, Morocco, IEEE, 2023, pp. 602–607.

[124] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A survey of deep learning and its applications: A new paradigm to machine learning," *Arch. Comput. Methods Eng.*, vol. 27, no. 4, pp. 1071–1092, 2020. doi: 10.1007/s11831-019-09344-w.

[125] H. Cui, T. Xue, Y. Liu, and B. Liu, "Transferable intrusion detection model for industrial Internet based on deep learning: IIDS model combining hybrid deep learning model and transfer learning," in *2024 3rd Int. Conf. Cryptography, Netw. Secur. Commun. Technol.*, beijing, china, Jan. 2024, pp. 107–113.

[126] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, K. Anoh, and A. A. Atayero, "SMOTE-DRNN: A deep learning algorithm for botnet detection in the internet-of-things networks," *Sensors*, vol. 21, no. 9, 2021, Art. no. 2985. doi: 10.3390/s21092985.

[127] A. Zaidi and A. S. M. Al Luhayb, "Two statistical approaches to justify the use of the logistic function in binary logistic regression," *Math. Probl. Eng.*, vol. 2023, no. 1, 2023, Art. no. 2715. doi: 10.1155/2023/5525675.

[128] B. Charbuty and A. Abdulazeez, "Classification based on decision tree algorithm for machine learning," *J. Appl. Sci. Technol. Trends*, vol. 2, no. 1, pp. 20–28, 2021. doi: 10.38094/jastt20165.

[129] A. Parmar, R. Katariya, and V. Patel, "A review on random forest: An ensemble classifier," in *Int. Conf. Intell. Data Commun. Technol. Internet Things (ICICI) 2018*, Springer International Publishing, 2019, pp. 758–763.
[130] K. Taunk, S. De, and S. Verma, "Machine learning classification with K-nearest neighbors," in *2019 Int. Conf. Intell. Comput. Control Syst. (ICCS)*, Secunderabad, India, 2019.
[131] M. A. Chandra and S. S. Bedi, "Survey on SVM and their application in image classification," *Int. J. Inf. Technol.*, vol. 13, no. 5, pp. 1–11, 2021. doi: 10.1007/s41870-017-0080-1.
[132] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022. doi: 10.1109/ACCESS.2022.3165809.
[133] P. Dini *et al.*, "Design and testing novel one-class classifier based on polynomial interpolation with application to networking security," *IEEE Access*, vol. 10, no. 11, pp. 67910–67924, 2022. doi: 10.1109/ACCESS.2022.3186026.
[134] E. M. de Elias *et al.*, "A hybrid CNN-LSTM model for IIoT edge privacy-aware intrusion detection," in *2022 IEEE Latin-Am. Conf. Commun. (LATINCOM)*, Rio de Janeiro, Brazil, IEEE, Nov. 2022, pp. 1–6.
[135] C. Hazman, S. Benkirane, and M. Azrour, "DEIGASe: Deep extraction and information gain for an optimal anomaly detection in IoT-based smart cities," 2022. doi: 10.21203/rs.3.rs-2141835/v1.