JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 5 No. 2 (2024) 110-136
https://publisher.uthm.edu.my/ojs/index.php/jscdm

A Comprehensive Review of Recent Types of Flooding Attack and Defense Methods in IoT-Based Smart Environments

Bashar Ahmed Khalaf[1]*, Siti Hajar Othman[1], Shukor Abd Razak[2], Alexandros Konios[3]

[1] *Faculty of Computing,*
Universiti Teknologi Malaysia, Johor Bahru 81310, MALAYSIA
[2] *Faculty of Informatics and Computing,*
Universiti Sultan Zainal Abidin, Kuala Terengganu 21300, MALAYSIA
[3] *Nottingham Trent University, Nottingham, UNITED KINGDOM*

*Corresponding Author: basharalzubaidy60@gmail.com
DOI: https://doi.org/10.30880/jscdm.2024.05.02.009

Article Info

Received: 19 May 2024
Accepted: 2 December 2024
Available online: 18 December 2024

Keywords

Flooding attacks, smart city, IoT, learning detection methods,

Abstract

In an attempt to completely transform people's lives, smart cities have implemented a collection of remodelings. Nevertheless, even though smart cities greatly enrich people's quality of life and provide significant convenience, there are still more unaddressed cyber security risks, such as malicious cyberattacks and information leaks. The efficient design of the defense model is crucial for safeguarding smart city cyberspace, as present cyber security advancements are not keeping up with the rapid uptake of these technologies worldwide. The present study describes in detail the architecture of a smart city and the sophisticated types of flooding attacks that could target it. Also, the study examines the current literature on IoT security in terms of smart cities that will provide an outline for the concepts of cyber security, learning-based defense methodologies. In particular, several learning methods were quickly examined to overcome the impact of flooding attacks, including Instance Supervised Learning (ISL), Sequence Learning, which is also supervised. On the other hand, the other variant of learning that is semi-supervised also introduced, sucha as the Reinforcement Learning and the Hybrid Learning. Additionally, the review illustrates the recent datasets that have been used to evaluate the efficiency of flooding defense systems.

1. Introduction

The population of metropolitan areas has been growing quickly in recent decades. Over 50% of people on the planet live in urban areas, according to United Nations Population Fund research [1]. The notion of a "smart city" has garnered excessive interest from both the academic and industrial sectors because of its stringent prerequisites and real-world application in an urban setting [2]. A number of towns have started to formulate their approaches towards the notion of smart cities in an attempt to improve citizen services and quality of life. Large sums of money are being spent on projects connected to smart cities in several populous nations. China is currently engaged in over 200 projects aimed at implementing the smart cities concept [3]. Urban municipals can now better manage their daily operations to advance people's value of life thanks to technologies related to smart cities. In order to help people in a range of applications such as smart parking, smart traffic systems, smart

healthcare, smart transit, smart agriculture, and smart homes smart cities' infrastructure consists of several interconnected systems and devices.

Packet delivery in unpredictable environments can be maintained using the networking paradigm known as information-centric networking (ICN). Consequently, ICN may be seen as a smart city substitute for IP-based networks [4]. IoT and its associated applications can be developed through the use of ICN solutions in addition to IP-based strategies like the one described in the work of Al-Turjman et al. [5]. Finding information at the heart of the architecture and labeling content accordingly, as opposed to relying on IP host identification, is known as information-centric networking.

Cities are becoming smarter, though, and this could put people at serious risk for privacy and security. This is because the smart city (SC) is prone to various security assaults because of the characteristics of devices with limited resources. Several hacks on SCs could be the result of these weaknesses. For example, by manipulating sensor data, hostile attackers may generate false data, leading to the loss of control over highly intelligent systems [6]. 230,000 people in Ukraine experienced a significant power outage in 2015 as a result of a denial of service (DoS) attack launched by hackers on the smart grid [7]. That is, the security and/or privacy of residents in smart cities may be in danger from a variety of resource-constrained devices, including cameras and sensors, which gather and exchange sensitive data.

These assaults have made it possible to expose people's private lifestyles and possibly cause financial loss by using home area data that smart homes collect and manage. Research projects that by 2020, the market for smart cities would have grown to a value of $1.5 trillion. In actuality, governments must draw significant funding so as to achieve the goal of smart cities [5]. Thousands of sensor nodes have been installed across the city as part of this enormous development to give residents access to real-time data on a variety of services, including public transit, traffic patterns, air and water quality, and energy consumption rates, to mention a few [8]. However, handling and examining the enormous volume of private information raises a number of security and privacy issues as well as worries about how to keep private information safe while it's being accessed by unauthorized persons [9]. Cloud computing can offer affordable services for data processing and storage in the Internet of Things (IoT) era and smart cities. individuals in intelligent cities.

However, the fog computing paradigm can address a number of problems with cloud-based IoT applications, including security, latency, location responsiveness, and deficiency of mobility availability [10]. By offering computer services to consumers at the network's edge, fog computing solves these issues by lowering latency and improving service quality [11]. However, because fog computing and cloud computing are different, security and privacy are difficult problems in fog computing. As a result, security solutions designed for cloud services are inapplicable to fog computing services that users can access. Numerous cryptographic methods are available to counter security breaches. Subsequently, the contributions of this study are summarized below:

- Layered designs for smart cities, security, and potential attacks against them are all examined and discussed.
- The study explores the sophisticated types of attacks that can target smart cities.
- The study offers incisive assessments and conversations on the early approval of conventional cutting edge defensive techniques, that fully realize the promise of IoT-empowered smart assets in smart cities,
- Thus, the work offers a thorough categorization and in-depth analysis of the most recent learning-based protection techniques to protect smart cities from sophisticated threats.
- Furthermore, the study categorically reviewed the recent standard dataset that has been created for testing and assessing the attainment of the planned protection schemes in the field of cybersecurity which has been done previously.
- The study outlined the benefits and drawbacks of the current protection strategies in smart city designs.
- Finally, the study provides IoT's-based smart cities latest significant achievements as well as proposals for its future concluding the paper in the final section.

This review paper presents recent trends in sophisticated flooding attack detection methods for IoT-based smart cities. The review covers more than a decade (11-years, 2013-2024). The keywords for the search are flooding attacks, DDoS attacks, IoT, smart city, software-defined network, machine learning (ML), and deep learning (DL), and reinforcement learning. The study included around 95 references, 7 review papers, 5 dataset online sources, and 83 research papers. The studied publications which are included in this review-work is shown in Fig. 1 based on the year of publication, and the "*" symbolizes the whole survey articles involved in this study in terms of year.

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 110-136

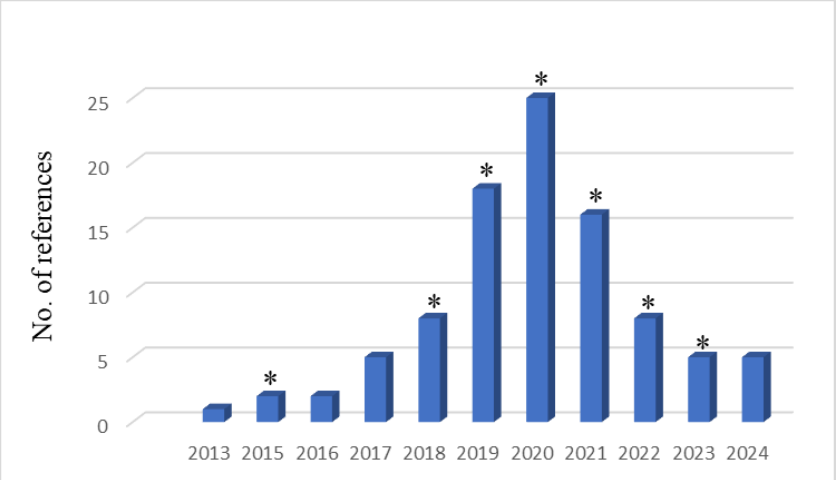


Fig. 1 *The outline of the reviewed articles*

The structure of this work is planned consequently as; Section 1 gives an summary of smart cities and it is applications, security, and threats have been presented briefly. Section 2 presents the related surveys. The smart background, layers, and security have been presented under section 3. Whereas, the sophisticated types of flooding attacks that could target smart city was illustrated in section 4. In section 5, the most effective learning-based defense methods were presented. Testing datasets that dedicated for testing and evaluating the functioning of the proposed smart cities defense techniques were presented consequently before the last section (section-6). Last but not least, the concluding remarks of the study are indicated in section 7.

2. Related Surveys

Internet of Things (IoT) smart assets provide unique security risks in smart city settings, according to multiple surveys. According to Ghiasi et al. [12], improvements in metering, smart control systems, communication networks, and Internet-based structures have led to moderate changes in new power system forms in various Cyber-Physical Power Systems (CPPSs). Connected in these constructions are cyber components and electricity sections. Some of the newly recognized challenges that CPPSs face include security, vulnerability, resilience, stability, and reliability. Precise modeling approaches and investigation of the interaction processes pertaining to the cyber-security of Smart Grids (SGs) are crucial for assessing, evaluating, and providing solutions to mitigate or eliminate these problems. This work attempts to review the relevant solution approaches for cyber-security in energy systems and methodically outlines various methodologies and procedures. We first go over the interactive aspects of cyber-security, after which their methods and models are thoroughly examined and compiled. Moreover, a technical discussion and analysis are conducted regarding the attributes and suitability of various cyber-attack models. The most recent research areas are presented, together with the state-of-the-art cyber security techniques—such as blockchain and quantum computing—in power systems and super grids. The effective strategies for resolving conflicts and safeguards are outlined.

Internet of Everything (IoE), Cyber-Physical Systems (CPSs), and IoT have all come to rely on smart gadgets, according to Khalil et al. [13]. In contrast, these blueprints for buildings lay the groundwork for realizing the concept of smart cities and, in the long run, a smart planet. Smart houses, smart grids, smart transportation, smart healthcare, smart agriculture, and other cyber-physical systems are all a part of smart city architecture. The network's periphery is where all of these real-world smart devices—sensors, aggregators, and actuators are linked. In order to make well-informed decisions, these gadgets collect data and use it to trigger actions. The security of these devices is crucial in this situation, especially concerning authentication, since the entire infrastructure would be at risk in the event of unauthenticated or malevolent assets. We classify centralized and distributed architectures to give an updated evaluation of authentication technologies. Further, the work is adopted to discuss the security concerns that are related to smart appliances and their authentications. Moreover, the work assesses and/or scrutinize the examination of suggested works systems that present difficulties with authentication concerning computational expenses, communication overheads, and models utilized to achieve resilience. Therefore, there is a pressing demand for lightweight solutions for handling, preserving, analyzing, handling and archiving authentication information for assets. Cloud computing has been quite helpful from an integration standpoint. On the other hand, there is still a great deal to learn about decentralized ledger technology, or blockchain, lightweight cryptosystems, and AI-based solutions. In conclusion, we go over the upcoming research difficulties that will eventually assist in resolving the unclear areas in need of improvement.

Vishwakarma and Jain [14], the thought of IoT has developed a significant innovation in utilizing wireless media's immense capacity in practical applications. By connecting with a multitude of intelligent programs that operate independently on various platforms, nearly anywhere in the globe, so that it could impact the planet around us. Considering how common it is, IoT frequently acts as a platform for the growth of malevolent organizations. By taking advantage of the Internet of Things vulnerabilities resulting from a number of limitations, such as inadequate security, scarce resources, etc., these entities are able to gain access to authorized devices and can launch a variety of attacks. The recent occurrences of notable servers being destroyed, which have been reported in the past few years, have made defending in contradiction of distributed denial-of-service (DDoS) outbreaks in the IoT an urgent field of research. To find the security holes in the different DDoS defense strategies, they are compared and given a general description. Additionally, we enumerate the uncovered studies problems and difficulties, which should be solved for more robust and intelligent DDoS protection.

The development of blockchain technology has been described in [15], taking into account blockchain platforms, consensus algorithms, and constituent technologies. The writers talk about the security risks associated with smart cities and offer a critical assessment of the different smart applications made possible by blockchain technology. To further reinforce the review, an employment constructed according to actual blockchain situation has been provided as a research piece. Looking at smart city integration of BC through an improvement lens, the assessment lays out the necessary prerequisites and research gaps. We have also evaluated and assessed the present security measures to better improve the detection of limits. The reliability and safety of CPS systems are ensured by a variety of security characteristics, offerings, and principles. The survey's recommendations and guidance are aimed for CPSs that are struggling with authentication, permission, and security services. The elements of the smart city to implement the idea are identified in the literature analysis [16]. The context of SCs is taken into consideration while discussing statistical analysis and real-world implementations. An analysis of these forthcoming investigate difficulties has been highlighted, outlining the prospects for progresses, since smart cities confront significant obstacles and issues because of the variety of smart assets and the massive data processing demands.

Mishra and Pandya [17], IoT technology is booming and permeating every aspect of our life, including healthcare, homes, cars, and education. Heterogeneity, scalability, quality of service (QoS), security needs, and many other issues are emerging with IoT technology as the number of connected devices rises. Due to factors including cost, size, and power, security management in IoT is subpar. Because consumers are wary of utilizing IoT devices due to security concerns, it presents a serious danger. In order to be prepared for the same, it compensates for the urgent need to evaluate current security threats and talk about impending difficulties. With a particular focus on Distributed Denial of Service (DDoS) attacks, the study offers a multi-layered analysis of several security vulnerabilities existing in the perception, network, support, and application layers of the Internet of Things. Due to their ability to bring down their targets, DDoS attacks pose a serious threat to the cyberspace. We go into great detail about the many kinds of DDoS assaults, how they affect IoT devices, their effects, and ways to mitigate them. This review effort focuses on Intrusion Detection models and compares them with Prevention models for mitigating DDoS attacks. Additionally, a variety of ML and DL approaches for malware detection and data pre-processing have been covered, along with the categorization of intrusion detection systems (IDSs), anomaly detection methods, and IDS models based on accessabel datasets. Ultimately, while debating the difficulties facing research, potential answers, and future directions, a more expansive viewpoint has been envisioned.

The investigation of Khalaf et al. [18] work is highlighted the strategies used to recognise, alleviate, and avoid DDoS attacks. Due to the attacks' frequent manipulation and change of their patterns, ports, protocols, and operation methods, it is necessary to dynamically assess their fundamental characteristics. The majority of suggested DDoS defense techniques have various shortcomings and restrictions. While some of these techniques use anomaly-based defense mechanisms that are exclusive to certain DDoS attack types and have not yet been used in open environments, others use signature-based protection mechanisms that are unable to detect new attacks. Consequently, a great deal of studies has been done on the application of statistical and artificial intelligence approaches in defense strategies to recognize, lessen, and stop these attacks. The most common forms of defense are the subject of this investigation against flooding attacks (FAs) that involve learning based defense methods. The review also presents the most effective and dangerous kinds of attacks, and testing datasets that are employed to examine and evaluate the functioning of the planned defense systems. Nonetheless, the article's main contributions are listed here.

Several review and survey studies have been established for flooding attacks, these studies focused on the attack strategy, attack defense methods, testing dataset, and evaluation methods such as [12], [13] – [17] and [18]. The review of Ghiasi et al. [12] studies the cyber-attacks and defense methods employed to improve the security issues in smart grid energy systems. Whereas, the review of Khalil et al. [13] emphasizes the application of Blockchain for IoT-Empowered Smart Strategies in SCs versus Centralized Authentication Architectures. The review of Vishwakarma and Jain [14] presents the influence of DDoS outbreaks and the defense methods in the IoT environment. The analysis study of Silva et al. [15] a brief overview of SCs, tracked by the attributes and

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 110-136

features, generic structure, composition, and practical employments of SCs. Lee and Lee [16] identify five critical IoT technologies necessary for the effective employment of IoT-based products and facilities, and they examine three categories of IoT applications for enterprises aimed at augmenting consumer value. Mishra and Pandya [17] examined various security concerns within the IoT layers: perception layer, network layer, support layer, and application layer, with particular emphasis on Distributed Denial of Service (DDoS) attacks. Khalaf et al. [18] concentrate on prevalent defense strategies against DDoS attacks that utilize artificial intelligence and statistical methodologies. Table 1 illustrates the evaluation consequences of our studies with the correlated literature, SC to Smart Cities, SDN refers to Software Defined Networks, and LBDM term refers to Learning Défense Methods.

Table 1 *The summary of the related studies*

References	IoT	SC	SDN	LDM	Recent Dataset	Sophisticated FA
Ghiasi et al. [12]	-	✓	-	✓	-	-
Khalil et al. [13]	✓	✓	-	-	-	-
Vishwakarma and Jain [14]	✓	-	✓	✓	✓	-
Silva et al. [15]	✓	✓	-	-	-	-
Lee and Lee [16]	✓	-	-	-	✓	-
Mishra and Pandya [17],	✓	-	✓	-	✓	✓
Khalaf et al. [18],	-	-	-	✓	✓	-
Our study	✓	✓	✓	✓	✓	✓

3. Background of Smart Cities

The increasing urbanization of the world's population has become a significant problem that requires attention. Only 30% of people on Earth lived in cities in the 1950s. By 2014, that percentage had risen to 54%, and by 2050, the UN projects that it will have reached 66%. China's urbanization rate increased from 40.53% to 53.73% in the past decade [19]. Cities and megacities (cities with a population of more than 10 million) are becoming more common as a result of the irreversible trend of urbanization. Urbanization causes a number of important and crucial changes in the economy, culture, manufacturing and demographics [20]. The process of urbanization has considerably enhanced people's standard of living by constructing sewage systems, housing and commercial structures, transportation, medical facilities, and educational. Cities serve as centers for regional economic development and job creation in their respective regions. Urban locations have a higher concentration of educated individuals, making the industrial organization more effective. Urbanization, however, also brings along new challenges and issues. Environmental and ecological issues are exacerbated in cities due to population growth and the intensive utilization of natural resources [21].

People now have the opportunity to minimize the severity of urbanization problems and/or find remedies as a result of the ICT revolution. In both of those places, there has been a fundamental change in governance during the previous ten years. They are becoming more and more information-based and computerized [22]. The Internet has largely taken over peoples' daily lives, and ICT has firmly melded with different directions, such as that related to the economics or that related to the citizen's cultures, it also involved to the life style and transportation, or the entertainments, and all other aspects of cities. The many accomplishments of digital transforming a city's statistics fetch day-to-day comfort to the public and lay the groundwork for further development of contemporary cities through infrastructure and data agglomeration [23]. Over the past ten years, a variety of different areas have adopted cutting-edge information technologies like cloud computing, data vitalization, mobile computing, and IoET. With the use of cloud computing, programmers can offer Internet services without having to invest a sizable sum of money in either the hardware or the personnel needed to run it.

An information explosion has resulted from the volume of data produced and processed on both online and offline platforms, and a new field called "big data" has been created to cope with it. This issue has prompted the necessity for a novel and more scalable tactics to extract insights from large amounts of data. Researchers/investigators may admission and development material on all characteristics of life anywhere, at any time, using mobile computing [24].

The notion of a smart city has garnered interest from governments, corporations, colleges, and organizations around the globe. Different parties have attempted to understand smart cities from their respective perspectives. In the early 1990s, the term 'smart city' arose for the first time, and academics have emphasized knowledge, revolution, and globalization in the development process [25], [26]. Since the announcement of IBM's Smarter Planet initiative in 2008, smart cities have received considerable attention. The concept of smart cities has grown and evolved since then. Six intelligent aspects to take into account were listed in another description by Sangaiah et al. [27]: economy, government, environment, society, movement, and living circumstances. One common

definition of a SCs is one that uses ICT to fashion a city (government, education, conveyance, etc.) extra intellectual and effective. The concepts and definitions of SCs are motionless developing, and at the moment, there isn't a consensus or clear definition among the diverse participants. To analyze and execute smart cities in practice, a more thorough characterisation of the axiom "smart city" is immobile wanted. Numerous nations and localities have created smart city projects to tackle the challenges and problems associated with urbanization.

The United States remained among the primary nations to establish a SC project in response to President Obama's smarter planet notions. The European Commission's Digital Agenda effort has been launched and has accomplished a lot to date (2015). The commission's agenda encourages SCs in Europe to have a matching SCs and Societies creativity, which concentrates on eco-friendly urban areas. Along with the enthusiasm from developed countries, developing countries have also actively pursued the movement toward smart cities [24]. Urbanization is happening far more quickly in underdeveloped countries in particular, which has led to significantly worse infrastructural issues. China has substantially invested in smart cities (both research and implementation), with more than 200 experimental smart cities, spending more than 2 trillion RMB in just 2015 to support its large urban population [18]. India announced plans to develop in excess of one hundred SCs with advanced association systems across the nation in 2014. Additional SC creativities can be exposed in previous works for the city and application level of SCs.

ICT is decisive to the development of smart cities. The advancement of resource configuration research and the direction of technological development in every smart city area is aided by top-level architectural research. IBM carried out the earliest architecture research. It provided a thorough introduction to how technology works, focusing on infrastructure and services rather than placing an overly strong emphasis on the value of city data. The necessity to combine the various features of the SC such as the government, residents, society, finances, and basic organization was considered by Xie et al. [22] in their work on smart city architecture. However, there was little discussion of technology. A structured comprehension of the technology required to build an SC has been gained through research into smart city architecture. The various definitions of SCs offered by stakeholders have resulted in a variety of styles. Pretty much any structure plan demonstrates how multidisciplinary technology is driven and enabled, especially in data processing technologies. The idea of a SC has made extensive use of a series of innovation in data systems, counting the cloud computing field besides the big data field as w information representation/vitalization, furthermore, it included the IoT structures and mobile computing [28]. These enabling technologies with a data focus are crucial in implementing smart cities.

As stated above, the notion of the SC originated by the issues and challenges brought on by the world's rapid expansion. It is very much supported and driven by today's modern ICT. Many countries and cities have adopted wonderful innovations from the vast body of research on smart cities. However, there are still several important problems that need to be resolved. With that said, the security of smart cities is one of these outstanding issues.

3.1 Smart Cities Security and Threats

Feeling safe and secure is the attribute of security. In smart cities, security pertains to the proactive steps required to protect the city and its citizens from harm caused by physical or information theft or other illegal access that could disrupt the system [17]. Smart city security is different from traditional security measures in that it requires innovative methods to safeguard the systems and applications while considering features like resource constraints, distributed design, and geographical dispersion. A figure of specific problems, such as inadequate communication, insufficient information, and privilege protection, can affect SCs.

The basic goal of SCs is for the purpose of delivering the necessary facilities continuously and without interruption. Additionally, the absence of any service could be disastrous. However, because smart cities integrate a variety of technologies, software, and hardware that are prone to incompatibility, they are vulnerable to numerous attacks. An attacker could use these vulnerabilities to their advantage and damage the physical environment [20]. The decentralized structure of SC, where plentiful miniature instruments (called sensors) and other source-constrained devices are combined, presents another area of vulnerability and makes them a prime target for attackers. Therefore, smart cities must implement the necessary controls and safeguards to guarantee the system's complete end-to-end security.

Due to the changing environment, internet connectivity, and layered design of smart cities, it isn't easy to establish a single and centralized security mechanism. Therefore, each participating layer must have a strong security mechanism protecting privacy and security. The following subsections briefly explain the attacks that happen at different smart city tiers. Additionally, two key issues linked to smart cities will be covered throughout this portion of text, including the countless types of sophisticated outbreaks and the best forms of resistance.

The Application, Network, and Perception layers comprise the three key components of SCs, as mentioned in the discussion above. Fig. 2 in the subsection below illustrates that numerous attack types could target the SCs in the aforementioned layer. The most sophisticated of these are:

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 110-136

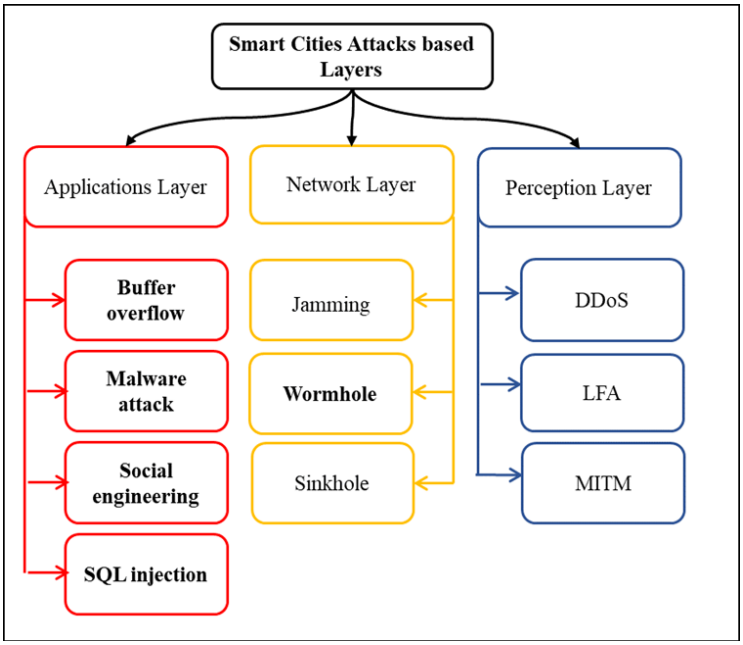


Fig. *2 Taxonomy of smart cities attacks*

3.2 Attack at the Application Layer

A top choice among crucial levels of smart city architecture is exchanging a significant volume of user data across different entities and applications. The majority of risks are those that will destroy the client's data, confidentiality, and illegal access to amenities are present at the application layer. In addition, the application layer, where, according on the QoSs provided, can be configured in multiple manners. According to [17], the common attacks at this tier include the following.

Hackers can use a software bug or vulnerability called a buffer overflow to break into company systems without authorization. Even though incredibly it is a widely recognized software security vulnerability, this problem remains quite pervasive and could have an impact on smart cities at the application layer. This is partially because buffer overflows can occur in many different ways, and the methods used to prevent them are typically error-prone [29]. The software error mostly affects buffers, meaning the consecutive bits of memory utilized to hold content as it travels from one location to another. A buffer overrun, or buffer overflow, happens when the amount of content being stored exceeds the capacity of the buffer. Overflowing into nearby memory regions, extra content either corrupts or overwrites what is stored there. An attacker launches a buffer overflow assault when he or she takes advantage of a programming mistake to do malicious things and infiltrate the system that is left vulnerable. In order to modify current files or leak data, an intruder changes the program's execution route and replaces portions of its memory [25]. As a means for obtaining unauthorized access to the network and resources, the attacker installs malicious software by taking advantage of the vulnerabilities [18].

After this, social engineering-based attacks appeared. "Social engineering" refers to a wide range of harmful practices that are carried out through interactions with individuals. Users are tricked psychologically into revealing personal information or committing security blunders. Attacks using social engineering may involve one or more steps. In order to prepare for an attack, a criminal first looks into the target to find out about possible points of entry and weak security [26]. Subsequently, the attacker attempts to win over the victim's trust by offering incentives to continue violating security, such as access to vital resources or the disclosure of personal information.

Web applications are vulnerable to SQL injection attacks, which permit malicious actors to alter database requests. As a general rule, it allows malicious actors to acquire information that would have been inaccessible to them else. Whatever information that the app has access to, including data from clients, might be included in this instance. An attacker can permanently alter the application's behavior or content by often updating or deleting this data [18].

3.3 Attack at the Network Layer

Data content routing and delivery are responsibilities of the network layer. However, this layer may experience radio interference, data leakage, and interruption issues because of the nature of the communication. In addition, at the network interface and service accessibility may also be exposed to threats by several security attacks. According to Ullah et al. [30], the frequent attacks that happen at this layer include a few types of attacks.

First is the Jamming attack. A common kind of assault is the jamming assault, especially in networks that are based on sensors, signal jamming negatively impacts communication that ultimately restrict the bandwidth availability [18]. Additionally, it is a subset of DoS attacks when malicious nodes intentionally disrupt networks to obstruct legitimate communication.

The second type is the Wormhole attack. A dangerous attack known as a wormhole attack involves two attackers intentionally positioning themselves within the network. Following this, the intruders keep listening to the network while capturing wireless information. Fig. 3 demonstrates the two attackers' advantageous network positioning.

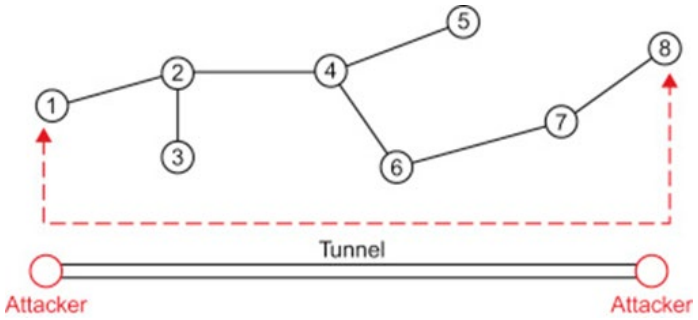


Fig 3 *The architecture of the Wormhole attack*

The attackers position themselves in the network in strong strategic locations, as was stated in the wormhole attack. They make use of their location, which is to say that, as shown in Fig. 3, they have the shortest route among the nodes. They publish their route in order to allow other devices/nodes in the network to realize it's the fastest way to transmit their data. In order to listen in on conversations taking place at one point in the network and redirect those conversations to a different one, wormhole attackers construct a tunnel [31]. The wormhole assailant at one side of the network accepts packets and transfers them to the other side of the network when the attacking nodes establish a direct link with one another. When this occurs, the attack is referred to as an "out-of-band wormhole".

Wormhole attacks include the attacker receiving packets at a single place in the network, tunneling them to an alternative place, and then replaying those packets back into the network. This attack could be conducted by tunneling each REQUEST directly to the target destination node in the case of reactive protocols like DSR and AODV. The neighboring nodes of the destination get this REQUEST packet. When they do, they follow standard protocol procedure to rebroadcast it and then ignore any subsequent REQUESTS for the same route discovery. Therefore, this hinders finding any other paths besides the wormhole [31].

The last one of the attacks is the Sinkhole attack. It involves luring nearby nodes with faked routing information, which is followed by selective forwarding or data tampering for data that passes through it. The attacking node asserts that it is providing a very attractive link. As a result, this node is bypassed by a lot of traffic [27].

3.4 Attack at the Perception Layer

Some devices function at the perception layer, such as GPS, tags, RFID, controls, and detectors/sensors. These devices have finite energy, computing power, and memory. Additionally, these devices are typically placed in hostile, open spaces where intruders could physically seize, tamper with, or even steal the keys. As a result, these devices are open to several attacks. The devices must be protected and the necessary precautions must be taken to reduce the likelihood of data leakage and the severity of any assault, Khalaf et al. [18] listed the typical attacks on the perception layer into i) DDoS Attacks, ii) LFA, iii) Coremelt Attacks, and iv) Crossfire Attacks.

DDoS attacks are carried out using computer networks. These networks consist of hacked personal computers (PCs) and other devices such as the Internet of Things (IoT), which allows hackers to take direct control of them [18]. These independent gadgets are referred to as "bots," and occasionally called "zombies," and a botnet is a collection of bots. An attacker can launch an attack by remotely instructing each bot in a botnet. When attacking a server or network, a bot in a botnet will query the target's IP address, which might cause the target to be overwhelmed and block genuine traffic [32]. Since every bot is a actually an Internet trick, it could be difficult to distinguish among legitimate and malicious communication [33].

One of the most devastating forms of assault on modern networks is the Link Flooding assault (LFA). The entire network might be brought to a halt by these assaults, which could choke crucial links due to a DoS [34]. Many LFAs have been extensively covered in the literature based on their respective methodology and tactics. These include crossfire, coremelt, and spamhaus. By overwhelming the surrounding lines with low-rate actual traffic, the crossfire LFA separates the victim and makes it more difficult to detect.

Nevertheless, this subsection describes different LFAs, such as the Crossfire, Spamhaus, and Coremelt Attacks. To demonstrate why crossfire attacks are the deadliest in contrast to all other attacks, we also compare these attacks based on several crucial characteristics for all LFA types. Attacks against network infrastructure have been much more frequent in recent years [18], [34], which increases the risk of cutting off a target area's network connections. LFA assaults are frequently conducted by sending an enormous amount of redundant requests to the goal machine or resource, disrupting the delivery of legitimate services.

The use of spoofed IP addresses by DDoS attackers makes it more difficult to identify the actual source of an attack. After a substantial amount of research into defending current networks, DDoS opponents have developed an advanced attack approach that uses stealth flows to target the existing networks. In line with this, the following subsections explain the various LFA types. The Coremelt attack, as seen in Fig. 4, involves the attacker using a group of compromised systems to flood a particular network link by sending packets to each other [35]. Moreover, because the assailants use the traffic-conforming protocol, they can avoid defenses based on flow filtering while communicating with other hacked systems through packet exchange.

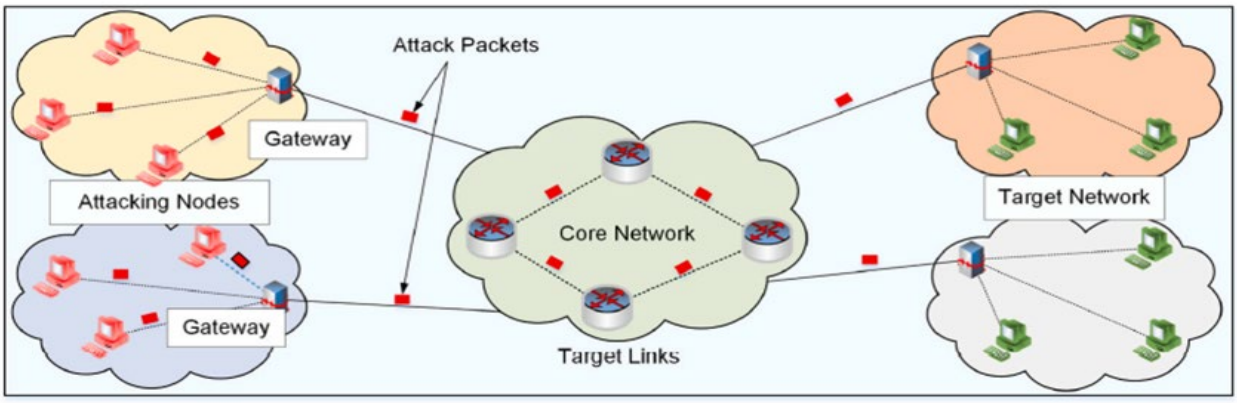


Fig. 4 *Coremelt attack architecture [36]*

Due to their ability to adjust to route alterations and avoid alerts by changing their intended connections following a predefined length of time, Crossfire assaults are additionally complicated and stealthy than Coremelt assaults. The competence is independent of the location of the bots, unlike the Coremelt attack, which does. Collaboration between ISPs is crucial for a successful defense that uses contemporary security apparatuses. When developing a strategy to lessen the impact, it is essential to keep all of these factors in mind. In a crossfire assault, automated programs direct traffic to dummy servers, which in turn block access to the real destination. Distributed, low-bit-rate traffic to disguises chokes the connections connecting the intended host to the network. While the target server is not frequently hit by flood traffic, detecting Crossfire LFAs is a tough task [37]. Similar to how bots employ real IP addresses, it is challenging to pinpoint the origin of an attack. After constructing a profile of the network and identifying the server being attacked and critical links to the attack, the primary action for the adversary is to send traceroute signals. It proceeds with selecting the decoy servers and calculate the necessary number of bot-decoy pairs to initiate the flooding activity. Lastly, it obstructs real traffic by flooding all paths to the target with low-rate streams sent by bots to decoys. By utilizing its indirect attack approach, there are multiple approaches in which the Crossfire assault might compromise the present SDN. Control channel LFA is an example of such a method.

The Spamhaus attack is a provider that sells subscribers spam filtering services. A significant Internet-scale LFA attack has been launched against the Spamhaus server. The attack was launched on several significant links, blocking cloud-based services at key Internet exchange points (IXPs) across Asia and Europe. Because of its extreme severity, this attack met the criteria for a certain kind of attack in LFAs. The attack first targets specific servers directly, but it developed and overwhelmed network lines on numerous IXPs over time. The Spamhaus server initially received service requests from attackers using open resolvers but was overwhelmed by the sheer volume and stopped responding. Later, Spamhaus deployed CloudFare's services to handle the massive attack load, which allowed the Spamhaus server to process queries [35]. The Spamhaus services were successfully shut down because of this strategy.

4. Learning Based Defense Methods

Several types of attacks may target Smart cities, with LFA being the riskiest. The most efficient and accurate attacks that have been conducted to counteract LFA will be presented and discussed in detail in this section. The first phenomenon to be discussed is Reinforcement Learning (RL), which belongs to a multi-agent system's

distributed computing (MAS). Each agent in the RL architecture is supported with sensing, acting, and learning capabilities. The learning of the agent performs instantly after executing the selected actions. More details about the RL are provided in Section 4.4.

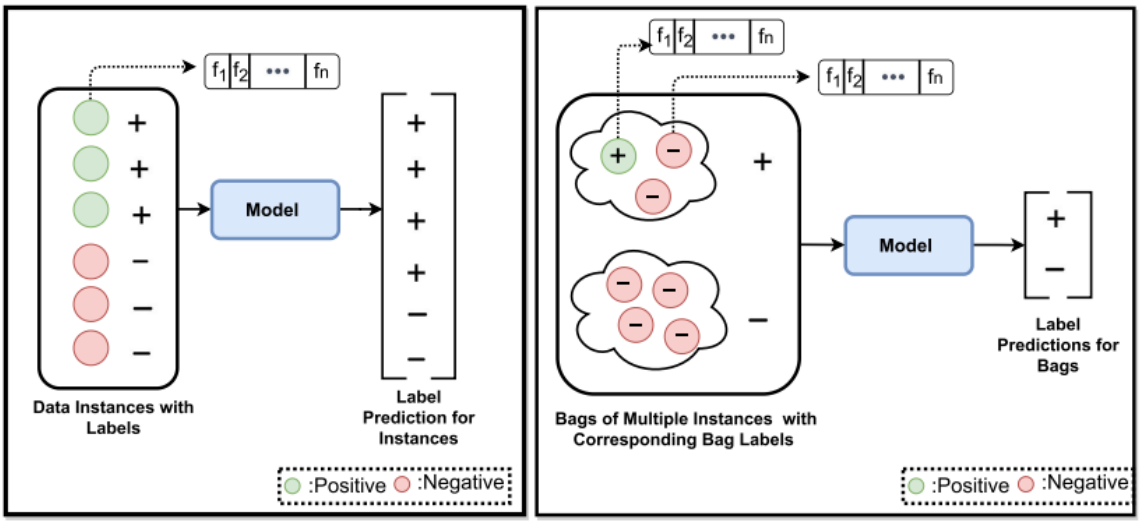
A branch of ML utilized in artificial intelligence (AI) named DL can learn through both supervised and unsupervised data. Due to the usage of multi-layer networks, DL is often referred to as deep neural networks or deep neural learning Aldweesh et al., [38]. Several studies have been done in attack detection and traffic classification such as Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Support Vector Machine (SVM), Logistic Regression (LR), K-Nearest Neighbors (KNN) and Gradient Descent (GD), according to the literature, it is observed that the best results reached when DL algorithm employed. The greatest popular and successful DL algorithms employed in the field of cyber security are presented in detail in this section.

Neurons connect the layers, symbolizing how the learning processes are calculated mathematically Goodfellow et al. [39]. On the other hand, DL algorithms take the pre-processed data as input, perform categorization and feature extraction, and then forecast whether the samples are benign or malignant. The taxonomy presents the most efficient learning bead methods that have the ability to achieve the best performance in defending against FA. These methods are divided into five groups: a) Instance and Multiple Supervised Learning, b) Supervised Sequence Learning, c) semi-supervised learning, d) Reinforcement Learning, and e) hybrid learning. However, the most effective learning-based defense methods that have been employed to identify and classify the flooding attack traffic have been presented and extensively reviewed in the following subsection:

4.1 Instance and Multiple Supervised Learning

Instance flow learning is one of the DL categories that has been used to classify network traffic. Moreover, an example of instance learning is deep neural networks, consisting of several layers that process the input data to outperform the output. [40]. They are a supervised learning technique. When compared to deep neural networks, CNN comprises two or fewer hidden layers [41].

When the expense of labeling each data instance is a significant barrier to annotation, this learning strategy is employed [40]. The multiple-instance learning (MIL) technique is one example of soft supervised learning. In MIL, the data are shown as many instances of bags with a single label per bag. In contrast to supervised learning, the training process does not have access to the instance labels. Instead of employing instance-wise labels for training, the MIL model uses weak bag-wise labels. Fig. 5 (a) and (b) depict the cases of supervised learning and MIL, respectively. The main goal of MIL is to create a model that uses training bags and matching labels to predict the test bag's label. The instance classification configuration used in DL, where each data instance is tagged, is demonstrated in Fig. 6 IL and MIL. The MIL bag classification method is displayed in b, where the instances are sorted into bags and given bag-level labels.



(a) Instance learning architecture **(b) Multi-Instance learning architecture**

Fig. 5 *The IL and MIL architectures [40]*

Depending on the level of classification granularity, the MIL techniques can be separated into two groups: bag-space level classification approaches, which train classifiers or calculate the distance between bags using the maximum margin approach; Simple single instance classification algorithms are applied in two ways: (1)

embedding-space classification, which converts a whole bag into a fixed-size vector representation; and (2) instance-space classification, which computes a score for each instance and determines the bag label based on the instance scores. Amaizu et al. [42], Since the actual positive instance within a positive bag, is often called the "witness" or the "key," the basic principle of MIL is that a bag is considered positive if at least one of its instances is positive.

Flooding Attack is one factor contributing to service degradation in the private cloud. The study by Virupakshar et al. [43], addresses distributed denial of service (DDoS) assaults that utilize connection and bandwidth flooding. Authors have utilized the DT, KNN, NB, and DNN algorithms to identify DDoS attacks in the OpenStack-based cloud. After comparing several classifier models, the authors chose the highest accuracy. Moreover, the Deep neural network model was employed because it has the best accuracy values when simulated and tested to a dataset that is generated dynamically. For cloud datasets, the DNN classifier achieved 96% accuracy and precision, outperforming DT, KNN, and NB. No details about the LAN and cloud datasets are given; the authors used the earlier KDDCUP99 dataset. For the KDDCUP99 dataset, the DNN method has an inferior precision score than competing techniques.

Deep neural network (DNN) architecture (i.e., Deep Detect) was introduced by Asad et al. in [44]. It has a feed-forward backpropagation design as its foundation. The authors developed this model to defend against DDoS attacks at the application layer. The CICIDS2017 dataset for DDoS detection is used to assess the suggested method. The approach has been compared with the RF and Deep GFL. With an F1-score of 0.99, Deep Detect surpassed the competing method. Furthermore, the extremely close proximity of the Area under the curve (AUC) value to 1.0 highlights the exceptional accuracy achieved by the proposed methodology. In order to protect applications from DDoS assaults, academics have implemented multiclass categorization and made it available online. So far, this tactic has been merely tried and true against application-layer DDoS assaults.

A flow databased DNN categorization algorithm to identify slow-rate DoS assaults on HTTP has been proposed in the study of Muraleedharan and Janet [45]. The proposed model used a deep network with FC feed forward. Then, to test and evaluate the performance of the proposed model, the CICID 2017 dataset with the features related to DoS and neglect the other features. The classifier can be used to identify the kind of DoS assaults. The model's overall accuracy in classifying attacks is 99.61%, according to the data. This approach is only used to evaluate HTTP slow DoS attacks (Slowloris, Slow rate HTTP traffic, and Golden Eye) using the CICIDS 2017 dataset.

In their prior work [46], Sbai and El Boukhari projected a DNN model that employed two hidden layers to identify the abnormal behavior of incoming traffic in MANETs. The authors employed the CICDDoS 2019 dataset to assess and test the suggested algorithm's functionality. According to the attained outcomes, the projected structure realized good functioning with an accuracy of 99%.

An effective approach for DDoS attack detection based on DL has been proposed by Amaizu et al. [42]. The proposed model is designed to work in 5G and B5G environments. Several steps have been taken to build the model, in the data preprocessing stage, the principal component analysis methodology has been employed in order to implement the feature extraction phase. Furthermore, the combination of two DNNs has been employed to identify the abnormal traffic and classify DDoS attacks. The suggested DNN architecture was successfully tested and evaluated using the CICDDoS 2019 dataset under various circumstances. The outcomes demonstrated that the model developed with DNN performed admirably, with a 99.6 percent accuracy rate.

Moreover, the Burst Header Packet (BHP) is another type of flooding attack that could be targeting the availability of the resource in the Optical Burst Switching network. Hasan et al. [47] claim that traditional ML algorithms cannot perform a good performance due to the small amount of the testing dataset. So, the writers have proposed a deep CNN structure. The outcomes have shown that the suggested scheme performed better for a given dataset with fewer features than the three ML methods. This multiclass classification was completed, and the model's effectiveness was assessed using 11 different performance measures. The suggested approach was evaluated using a dataset that is constructed of fewer instances and does not involve all sorts of traffic instances.

An improved DL model called Vector Convolutional Deep Feature Learning (VCDeepFL) has been proposed by Amma and Subramanian [48] to identify and classify the flooding traffic that belongs to DDoS attacks. The model consisted of two main stages: a) splitting data made into two parts, the training and testing part, and b) training and testing by the proposed DNN model. The NSL-KDD dataset was utilized to test and evaluate the suggested strategy functionality. Conclusions drawn from the findings show that the suggested approach outperformed the relevant studies.

Shaaban et al. [50] proposed the CNN model as a method for detecting DDoS doses. Thus, in this work, they employed a couple of two datasets. In the beginning, they employed the first dataset, which was manually generated, and the second dataset is the NSL-KDD. Both of them can simulate the network traffic to evaluate their suggested model with classification methods that belong to machine learning. Based on the observations, the suggested model performed admirably, achieving a 99% accuracy rate on both sets of data, outperformed the other machine learning algorithms that perform the classification process, which comprise the Decision Tree, Support Vector Machine (SVM), and Neural Network (NN). Whereas, the data was preprocessed and transformed

into a matrix by using a one-column padding to be readable by the proposed model. Therefore, it may influence how the model learns.

A deep CNN model for DDoS attack detection and classification in Software Defined Networks was proposed in the earlier work of Haider et al. [50]. The CICIDS2017 dataset has been used to evaluate the suggested ensemble approach. This approach is contrasted with the most advanced deep learning ensembles and hybrid approaches, including reinforcement learning (RL), long short-term memory (LSM), and recurrent neural networks (RNN). The CNN model achieved the good performance when it comaired with the other DL techniques. Additionally, the study has been contrasted the suggested collaborative CNN method with rival strategies. According to the obtained results, it is observed that the CNN model outperformed the rival approaches that are currently in use. Together, CNN achieved a 99.45% accuracy rate. This approach necessitates more time for testing and training than other methods. The mitigation mechanism can be affected as a result. As a result, attacks can cause more damage.

Using distributed tracing to monitor the behavior of the application as a whole and by computing the frequency distribution of unique traces to identify the unusual activity of a cyberattack, Jacob et al. [51], analyzed cyberattacks that targeted microservices applications. A microservice call graph is a decentralized trace that stores the API calls connecting the different parts of a distributed service. In this graph, the nodes are the microservices themselves, and the edges are the calls that go to specific microservices. The spatiotemporal properties of a microservice application's API call traffic may be represented by a series of these call graphs throughout time. The next step is to use graph-based anomaly detection to find differences in the application call flow that indicate strange or abnormal behavior.

In order to provide appropriate traffic management, it is essential to have accurate and up-to-date traffic forecasts, but traditional statistical techniques such as linear regression are not suited for this task (Yu et al., [52]). The traffic domain's time-series-based forecasting problem was modeled using a STGNN. The road portion of the network was graphed using convolution layers to enable quick STGNN training and to capture spatial and temporal features. Experiments utilizing several real-time traffic data sets showed that this technique readily converges and operates better than the starting point scenarios, which are state-of-the-art approaches.

In order to detect DDoS assaults, Chen et al. [53] proposed a system called DDoS Attack Detection using a Multi-channel CNN (DAD-MCNN). The amount of channels is also dependent on the attribute cluster count. The investigators have classified the features under multiple tiers, including packet, host, and traffic. The researchers used a progressive training strategy to train the DAD-MCNN. The suggested framework has been tested and evaluated using two datasets, namely KDDCUP99 and CICIDS2017. Neither the multi-channel nor the single-channel designs yield noticeably different results. Additionally, the multichannel models' sophistication will increase, which can render them unfit for validation in situations that occur in real-time. The results of the FA traffic supervised instance learning are summarized in Table 2.

Table 2 *The summary of supervised instance learning for FA traffic*

Ref.	Model	Evaluation	Dataset	Advantage	Disadvantage
Virupakshar et al. [43]	DNN	Precision	KDDCUP99	It can dynamically capture and process the Network traffic.	It has only been tested to identify DDoS assaults in OpenStack private clouds.
Asad et al. in [44]	DNN	Accuracy	CICIDS2017	It can also identify harmful activity from packets when a brand-new malicious pattern is applied. It can repeatedly identify large-scale trends in network traffic.	It can only detect limited types of flooding attacks.
Muraleedharan and Janet [45]	Deep Neural	Accuracy	CICIDS2017	It efficiently detects and prevents a low rate of DDoS attacks at the application level.	It can only detect DDoS attacks at the application layer level.
Sbai and El Boukhari [46]	DNN	Recall, precision, F score	CICIDS2019	It is efficient in detecting data UDP flooding attacks in MANET	It can only detect limited types of flooding attacks. It is tested only in the MANET network.
Hasan et al. [47]	Deep CNN	Accuracy, Sensitivity, Precision,	BHP on OBS dataset	It is effective in automatically detecting the BHP flooding attack at edge nodes	It is challenging to categorize the issues with various network attacks.

Amma and Subramanian [48]	VCDeepFL	Accuracy	NSL KDD	I can efficiently identify and detect DoS attacks with good accuracy.	The model was not dialed with the huge number of DDoS traffic.
Shaaban et al. [49]	CNN	Accuracy	NSL-KDD	With a 99 percent accuracy rate, the suggested model can identify and categorize DDoS traffic into harmful and legitimate data.	The model cannot block or mitigate DDoS attack
Haider et al. [50]	A hybrid of CNN and RNN	Accuracy	CICIDS2017	To solve the problem of detecting the most common and advanced DDoS attacks in SDNs, the approach is effective and scalable.	The proposed system not test yet with a real traffic data.
Jacob et al. [51]	Distributed tracing-based ML	Qualitative	Created dataset	It can detect cyber-attacks at an early stage	The proposed system not test yet with a real traffic data.
Yu et al. [52]	STGNN	Time Consumption	Real-world traffic	With flexibility and scalability, it achieves fewer parameters, easier convergences, and faster training.	It can only detect limited types of flooding attacks.
Chen et al. [53]	DAD-MCNN	Accuracy	KDDCUP99 and CICIDS2017	The model can identify DDoS traffic with good accuracy	The complexity of validation will rise in real-time circumstances.

4.2 Supervised Sequence Learning

Gamage and Samarabandu [40], presented Supervised Sequence Learning, an early framework for supervised learning on sequences. It is a feedforward network that has additional special units added to its single hidden layer. Values from the output nodes are sent to the special units, which at the next time step transmit these values to the concealed nodes. The special units enable the network to recall actions performed at earlier time steps if the output values represent actions. A series of flows is used in supervised sequence learning [40]. This type of model, as shown in Fig. 7, remembers the previous input states while learning from a series of inputs.

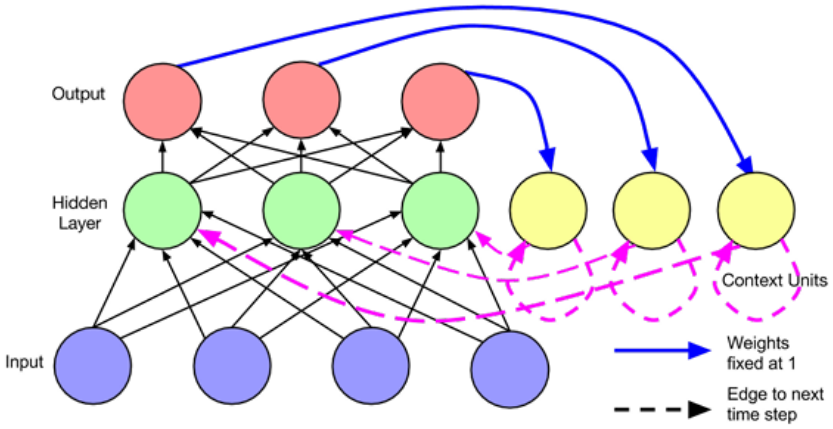


Fig. 7 *The architecture of the SSL as proposed [54]*

However, this section has provided the following list of supervised sequence learning techniques: Recurrent neural networks (RNNs), which consist of three main layers (input, hidden, and output). These layers work together in the feed-forward architecture to exploit prior information [54]. Therefore, guessing what word will come after another in a phrase is improper. The RNN may anticipate the following word in a phrase by recalling earlier information, as the output from the preceding phase is passed to the currently running step together with the present input. However, the RNN has shortcomings, including problems processing big sequential data and gradients disappearing or exploding.

Nisha's work, however, clearly shows that the LSTM has overcome the RNN issue. The memory cells or blocks that make up the LSTM network are diverse. The current state of the cell as well as its concealed state are sent to the subsequent cell. Input, output, and gates forget allow the memory blocks to choose what to remember and what to discard. The LSTM removes unnecessary cell state data using the forget gate. By analyzing the present state of the cell, the output gate extracts essential details and treats it as an output. To the contrary, data is added to the cell state by means of the input gate.

The most well known DNN algorithm which called RNN that perform the classical NN that consists of three processing layers (input, hidden, and output) layers has been proposed in this study. Because the process of inputs and outputs are autonomous for each other, feed-forward neural networks are unable to exploit prior information [54]. Therefore, it is improper to guess what a phrase's next word will be. The RNN may anticipate the following word in a phrase by recalling the prior data, as the output from the preceding phase is passed to the present phase together with the present input. Nevertheless, the RNN has shortcomings, including problems with gradient expanding and disappearing, as well as problems with massive amounts of sequential data. But Nisha's work clearly shows that the LSTM has solved the RNN problem. Different memory cells or blocks make up the LSTM network. The forget, input and output gates are the three mechanisms that provide the two states—hidden and cell states—to the subsequent cell. The information that the memory blocks choose to retain or forget is up to them. The forget gate eliminates cell state data that the LSTM is no longer in need of. The current cell state is processed by the output gate, which is responsible for extracting relevant details from it. In contrast, information is added to the cell state by means of the input gate.

The Diffusion Convolutional Recurrent Neural Network (DCRNN), a recently designed GCNN, is a cutting-edge model created for understanding the intricate spatial and temporal aspects of traffic flow. The use of spatiotemporal traffic forecasting in the context of road networks was described by Li et al. [55]. On a directed graph, they suggested modeling the traffic as an active diffusion process. Future traffic patterns are predicted after learning the ground truth observations. Two distinct databases that contained actual traffic from real-world road network traffic were used to test this method. The first data collection includes traffic information gathered over four months from 207 sensors dispersed around Los Angeles County. This framework was put to the test, and it was found to perform 12% to 15% better than modern standard frameworks.

Published in [56] was a deep learning approach for detecting DDoS assaults in an SDN setting. The model consists of input, output, FC hidden layer, forward, reverse, and recursive layers. In the model, RNN, LSTM, and CNN were also utilized. As a result, the authors have developed four distinct models: first is based on LSTM structure, second based on CNN layers which is combined with LSTM, and those based on the GRU structure. The ISCX dataset has a 98% accuracy rate when used to predict a DDoS attack. The ubuntu14.04 operating system is used to build the DDoS attack detection and defense system, and the DDoS defense system is tested using real DDoS attack traffic.

An RNN model for identifying and classifying anomalies traffic has been proposed by Liang and Znati [57]. This model directly infers network traffic behavior from a short packet sequence, eliminating the requirement for manually created feature engineering. This study conducted three trials using three additional algorithms (DT, ANN, and SVM) using the Wednesday and Friday CICIDS 2017 datasets. By learning the complex flow-level feature descriptions inherent in the raw input, the LSTM-based technique outscored competing tactics, as demonstrated by the findings of study no. 1. The second experiment demonstrated that the suggested method had the ability to record the ever-changing patterns of an unidentified type of network data. Experiment 3 found that, even with higher n values, allowing the model to test more packets for each flow does not necessarily improve the performance. Over unknown traffic, the suggested strategy performs better than the conventional machine learning techniques. The suggested model employs a subsequence of n-packets, such as the $S \subset F$. S is padded with fake packets when a flow is short on packets. The proposed model's learning process and functionality might be affected through these padding settings.

The authors of the study by Liu et al. [58] first create a game model to examine the advantages of attack for both attackers and defenders. It is important to make the defender manage expired state entries during stateful forwarding in order to increase the defender's utility further. An improved Distributed low-rate Attack Mitigation (eDLAM) mechanism has been put forth in order to achieve this goal. In particular, eDLAM keeps an extremely small malicious request table to relieve stress on the practical forwarding state table (MRT). In MRT, a packet request that matches will be immediately flagged and dropped, with no effect on the forwarding state table. In order to maximize defender usefulness, eDLAM uses an ideal threshold updating technique for MRT based on this. We evaluate the eDLAM performance's false positive rate (FPR) and false negative rate (FNR). Extensive experimental data shows that eDLAM can reduce FPR by 44% and FNR by 10.5% on average when compared to state-of-the-art techniques.

Graph Neural Networks (GNNs) have emerged as the cutting edge of DL research in recent years, demonstrating cutting-edge performance in a variety of applications Wu et al., [59]. Data that is graph-structured and consists of objects (i.e. nodes), and relationships between objects (i.e., edges) are quite common. Graph-level learning is the study of a variety of graphs rather than just one. The norm used to be the traditional graph-level

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 110-136

learning method. However, due to their superiority in modeling highly dimensional data, Graph-level Neural Networks and DL-based graph-level learning approaches, have gained popularity as the scale and complexity of graphs have grown. According to the obtained results, it is observed that the proposed model achieved a good detection accuracy during the comparison with the related work.

Shurman et al. [60] proposed two techniques to detect DoS/DDoS attacks: an LSTM-based DL model and a hybrid-based IDS. It has the capability to block any unwelcome Ips. The LSTM model, which was utilized in the second method, was trained using a variety of DDoS attacks from the CICDoS2019 dataset. Other models that are currently in use are compared to the second model. The results show that the model performed better than alternative models. On the reflection-based CICDDoS2019 dataset, the LSTM-based model displays an accuracy of 99.19%. However, only the reflection-based CICDDoS2019 dataset has been employed in the study. Additionally, there is no interdependence between the hybrid IDS and LSTM approaches.

In the article by Assis et al. [61], an SDN environment that protects over DDoS and intrusion danger was put forward. The detection and mitigation modules make up the two key components of the suggested system. The role of the detection module is to detect attacks. By examining individual IP traffic records, the developers of this module have applied the DL-based GRU approach to identify DDoS and intrusion attempts. The mitigation module responds to attacks that are detected by taking appropriate action. The CICDDoS 2019 and the CICIDS 2018 datasets have been compared by the authors using their proposed model to seven different machine learning algorithms. These many machine learning and deep learning techniques include KNN, RNN, DNN, CNN, GD, and LR. The authors used the CICDDoS 2019 dataset as their first test case and the CICIDS 2018 dataset as their second. The authors have evaluated the suggested model with other ML approaches in terms of their precision, accuracy, and f-measure, as well as the efficiency of the approaches' classification of normal and attack flows separately using both datasets. The outcomes demonstrated that in all these test cases, the GRU was capable of detecting DDoS and intrusion attacks. CICDDoS 2019 and CICIDS 2018 datasets have been used to test and evaluate the proposed system's performance. According to the obtained results, it is observed that the proposed model achieved good results with an accuracy of 99.94%. Table 2 presents the analysis of the Supervised Sequence Learning.

Table *2 The analysis of supervised sequence learning for FA traffic*

Ref.	Model	Evaluation	Dataset	Advantage	Disadvantage
Li et al. [56]	RNN	Accuracy	The ISCX dataset	The model can track past network assault activity and identify patterns in network traffic sequences. The model is efficient in detecting DDoS attacks in a real environment	The model does not deal with LFA
Liang and Znati [57]	LSTM	Accuracy	CICIDS2017	Attack traffic's dynamic tendencies can be captured by it.	The model was not tested with a real dataset
Liu et al. [58]	eDLAM	False negative rate and false positive rate	Generated dataset	The model can mitigate the low-rate attack with high accuracy and low false alarms	High complexity and high latency
Wu et al. [59]	GNNs	Accuracy	Generated dataset	The GNN is efficient in identifying and classifying abnormal traffic.	It is challenging to categorize the issues with various network attacks.
Shurman et al. [60]	a hybrid-IDS based on LSTM	Accuracy	CICDoS2019	The model is efficient in detecting suspicious network traffic from any network nodes	It can only detect limited types of flooding attacks.
Assis et al. [61]	DL-based GRU approach	Accuracy, recall, precision, and f-measure	CICDDoS 2018, 2019	This methodology facilitates expeditious mitigation reactions, hence mitigating the adverse effects of the SDN.	The model does not consider to work with time goes.

4.3 Semi-Supervised Learning

Deep learning research has found an interesting new direction in semi-supervised learning (SSL). These techniques address scenarios in which there are a large number of unlabeled data and few labeled training examples. In a situation like this, SSL techniques are better suited for real-world uses because labeled instances are frequently difficult, costly, and time-consuming to obtain, whereas unlabeled facts are easily accessible and accessible. Better classifiers can be constructed by SSL to make up for the deficiency of labeled training data.

In order to add more branches to any feed-forward network that performs well on supervised data in order to make use of more unlabeled data. The usage of Ladder Networks with an extra encoder and decoder for SSL is suggested by Rasmus et al. [62]. The network is made up of a decoder, a damaged and clean encoder, and two encoders, as shown in Fig. 6. Both encoders process the input x at each training iteration.

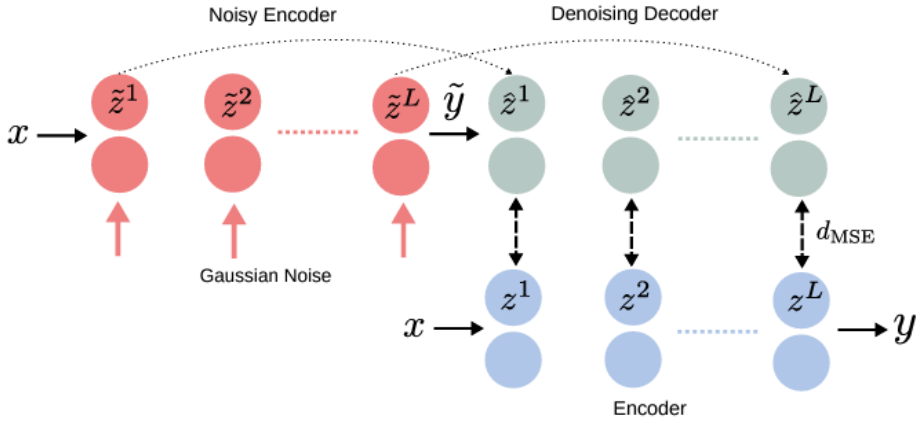


Fig. 6 *The architecture of SSl [62]*

However, the method can be easily adapted for deep learning algorithms by changing the fully connected layers with the layers of them for semi-supervised vision tasks. Furthermore, many studies have been well established by employing the SSl-based deep learning algorithms, the most effective of them have been presented below.

It employs the pre-training stage using unlabeled data. Training a model utilizing both labeled and unlabeled records is what this learning method is all about [40]. In this case, an autoencoder was employed for feature extraction, then identifying and classifying the attack traffic by using the DNN algorithm. A deep neural network known as dimensionality is employed for feature extraction and dimensionality reduction, according to Aldweesh et al. [46]. An AE technique has been utilized to process the data, and it consists of two processing stages, encoding and decoding. However, the encoding is considered the input, whereas, the decoding is considered as an output. Then, AE uses backpropagation training to train the encoder and decoder collectively. After collecting the raw characteristics from the input, the encoder converts it into a low-dimensional abstraction. The decoder then uses the low-dimensional idea to rebuild the original characteristics.

Catak and Mustacoglu suggested a deep ANN and an AE model combo [65]. The model's AE layer picks up the way to depict network flows. Furthermore, the DNN model attempts to pinpoint the precise class of anomaly traffic. Using the UNSWNB15 dataset and KDDCUP99 dataset, the authors tested their model using various activation functions. The best F1 result (0.8985) obtained was with the ReLu activation function for soft plus, soft sign, ReLu, and tanh activation functions. According to the obtained results, it is observed that the proposed model achieved a good performance during the comparison with the related work with an accuracy of 99%.

The proposed model's detection time is not computed because of its complexity, and it may take time to react to attacks, which can seriously harm the system. A five-layered AE model has been developed by Yang et al. [66] for efficient unsupervised DDoS detection. The detection model can be built by simply using normal data. The model then does the job of dividing the traffic into an attack and normal traffic. Through tests using various datasets (such as public datasets and synthetic datasets), according to the investigators, it is not possible to apply what one learns in one network setting to a different one. More importantly, this study proved that DT, a supervised ML method, is not good at detecting novel assaults that aren't in its training set. Despite this, the AE proved effective in countering both known and unknown threats. The authors also showed how AE-based DDoS attacks have negative effects on detection. On the datasets, the 16 features chosen with PCC and the 27 features in the AE-D3F framework performed similarly, although the former used fewer features. By training the algorithm with only regular traffic, this strategy makes up for the absence of marked attack information. Both feature learning and traffic categorization make use of it. Information is categorized according to the RE threshold

quantity. Even while testing against both known and unknown threats, AE-D3F manages to attain almost 100% DR with less than 0.5% FPR. Nevertheless, a number for the RE threshold has to be defined.

In the previous work of Kasim [67], the AE-SVM approach for classifying DDoS traffic has been proposed. The following test scenarios were used by the authors to evaluate their proposed model: a) The model was trained with 16,902 data; b) It was tested with 15,000 randomly chosen data from the CICIDS dataset; c) It was tested with 6957 datasets of DDoS attacks produced by the Kali Linux environment; and d) It was trained using the NSL-KDD train dataset with ten-fold cross-validation, and finally e) It was tested with NSLKDD. AE-SVM outperformed various other approaches in terms of minimized false-positive rate and rapid anomaly finding. The accuracy of the model that was suggested utilizing the data set from NSL-KDD is lower compared to that of the other two datasets.

In the study was done by Bhardwaj et al. [68], the authors proposed a deep learning model that integrates both stacked sparse AE and Deep Neural networks. The stacked sparse AE is employed to train the model and analyze the dataset then extract the features, whereas, the DNN employed for identifiyeng and classifying the attack tarffics. First of all, the authors used the random hyperparameter values for both AE and DNN in the Naive AE and DNN baseline model. Then, the AE and DNN were optimized for future AE and DNN model enhancements. The ten cutting-edge methods have been contrasted with the suggested method. The CICIDS2017 dataset was analyzed with the following strategies: decision tree analysis (DT), Artificial Neural Networks (ANN), Support Vector Machines (SVM), SAVAERCDNN, and Long Short-Term Memory (LSTM). The findings demonstrated that the proposed method achieved competitive outcomes with the CICIDS2017 dataset, attaining an accuracy of 98.92%, and surpassed existing methods with the NSL-KDD dataset, achieving an accuracy of 98.43%. The proposed method effectively resolves the challenges of feature learning and overfitting. The autoencoder is learned using random training data samples for feature learning, and the overfitting problem is mitigated by utilizing the sparsity parameter. This research has conducted offline analysis but has not yet assessed the latest dataset. The detection time for the suggested model has not been computed.

The Deep Learning-based Defense Mechanism (DLDM) paradigm is applicable to nodes with minimal or no mobility; nevertheless, in Wireless Sensor Networks (WSN), nodes exhibit significant dynamism and frequent movement. Furthermore, the generated dataset has been utilized solely for model assessment. Premkumar and Sundararajan [69] proposed a DLDM framework for detecting DoS threats in wireless sensor networks (WSNs). The authors employed the DLDM framework, which uses RBF-based neural deep learning to categorize data. The authors used NS2 to reproduce the experiments using the simulation parameters, and they then provided the detection performance with a single CH. The detection ratio is between 86% and 99% when a single CH is used, while the average false alarm rate is 15% when the number of attackers is between 5 and 15%. The DLDM displayed a greater detection rate and a lower false alarm rate for the whole data forwarding period than the MAS. Due to the nodes' decreased energy use, their lifetime is increased. On the simulator NS2, the suggested model's feasibility was evaluated by computing PDR, energy use, and throughput. Moreover, the proposed model is appropriate for nodes that move less frequently or not at all; however, the model's evaluation only used a generated dataset. Table 3 shows the summary of studies related to semi-supervised learning.

Table 3 *The summary of semi-supervised learning for FA traffic*

Ref.	Model	Evaluation	Dataset	Advantage	Disadvantage
Catak and Mustacoglu [65]	deep ANN and an AE	Precision Recall Accuracy	KDDCUP99	It can avoid overfitting to predefined malicious patterns.	It can only detect limited types of flooding attacks.
Yang et al. [66]	Auto Encoder based DDoS attacks Detection Framework	DR and FPR	Synthetic datasets	It can characterize typical traffic patterns utilizing an AE model. It can distinguish attack traffic from normal traffic based on reconstruction flaws.	The model is not considered to work with time. The model is not able to deploy in DDoS open threat signaling environments
Kasim [67]	AE-SVM approach	Accuracy	CICIDS and NSL-KDD	It provides better anomaly detection. It possesses considerable potential for real-time DDoS intrusion detection, particularly in the context of	It can only detect limited types of flooding attacks.

				imbalanced and unlabeled datasets.	
Bhardwaj et al. [68]	A hybrid of AE and DNN model	accuracy	CICIDS2017 NSL-KDD dataset	The system has achieved a good result in detecting FA	The system has not been tested with real-time traffic flows The system is not tested with big real-time data.
Premkumar and Sundararajan [69]	DLDM framework	accuracy	Generated dataset	It is adept at detecting and isolating attacks during the Data Forwarding Phase.	It can only detect limited types of flooding attacks.

4.4 Reinforcement Learning

Reward-based problem solving can be generally approached using reinforcement learning (RL). RL aims to replicate how humans pick up new skills through interaction with their surroundings rather than from an instructor. A subfield of machine learning called reinforcement learning (RL) looks at how the software agent's technology works in each situation to optimize the concept of cumulative reward. Since RL does not need the presentation of labeled input/output pairings or the intentional correction of undesirable actions, it falls under the category of unsupervised learning. Rather, the focus is on finding a balance between exploration (of unknown terrain) and utilization (of existing information). A basic RL design is shown in Fig. 7.

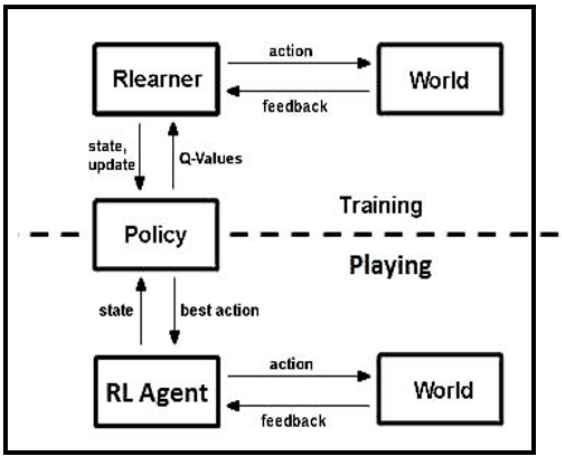


Fig. 7 *RL architecture [70]*

Zhang et al.'s study [71] proposes a novel reinforcement learning-based DDoS mitigation technique that shifts cloud filtering services to edge servers. Using classifiers, the edge servers are placed at different router sites and filter the incoming and outgoing traffic. A unique deep reinforcement learning framework is created to minimize attack traffic, reserve user traffic, and minimize inspection delays by balancing the deployment of computer resources and task allocation. The network structure information transformation is coded as a vector using a graph neural network, and the traffic data is fed into Q-Network to get the best allocation outcomes. The performance of the proposed technique is also tested and evaluated using the KDD19 dataset based on time consumption parameters.

Feng et al. [72] create a lightweight, statistically-based unsupervised classifier and suggest a novel collaborative DDoS detection technique based on reinforcement learning. Also, the authors install the classifiers in IoT edge gateways and use real-time network traffic feature analysis to find anomalies. We employ the soft actor-critic (SAC) reinforcement learning model, which is installed on the edge server, to adapt the underlying unsupervised classifier's parameter configuration dynamically in order to handle the IoT environment's fluctuations. This approach can guarantee superior detection performance for a variety of IoT device kinds. Furthermore, an edge server's collaborative aggregation module is built to exchange observation states and past experiences. It features a special collaborative reward system that enables the reinforcement learning model to utilize the collaborative work potential fully. Experiments conducted on a public data set and a built-in real-world

testbed show that our suggested solution has outstanding detection performance, particularly in properly identifying IoT-based DDoS attacks that are stealthy.

The proposal for Deep Adaptive Reinforcement Learning for Honeypots (DARLH) was made in the earlier work by Veluchamy and Kathavarayan [73]. In this honeypot setting, the suggested DARLHs system combines Deep Recurrent Neural Network (DRNN) and Intrusion Detection System (IDS) agents with Deep Adaptive Reinforcement Learning (DARL) to observe DoS attacks with multiple run times. For efficient runtime attack detections, the system develops DARL and DRNN IDS agent integration modules at the next stage. Python 3.7 is used to execute the method. The experimental results are compared with several contemporary approaches, including Recurrent Neural Network-based Signature Generation and Detection, Game and Naïve-Bayes Honeypot, and BlockChain Honeypot. The suggested approach is contrasted with the current approaches for DoS assaults, web attacks, botnet attacks, internal DoS attacks, brute-force attacks, and external DoS attacks. Based on the comparison, the suggested approach produces results that are 5%–10% better than those of another approach. Finally, the test results show that the performance of the suggested solution works best with another existing system.

The authors of Li et al.'s study [74] use reinforcement learning to present the FAST feature adaptation reinforcement learning strategy for DDoS mitigation, which is based on space-time flow regularities in IoV. To improve the speed and accuracy of DDoS attack detection in FAST, we have carefully designed a combinational action space and a reward function based on the Kalman filter technique and historical data traffic patterns. Then, by merging DDQN and Q-learning, FAST is able to choose features and disconnect DDoS attacks in a way that adapts to changes in the surroundings. We assess FAST's performance experimentally using the Shenzhen taxicab dataset. We use the DDoS simulation programs "ddosflowgen" and "hping3" to mimic and introduce DDoS attacks into Shenzhen taxis. In comparison to other detection techniques, the experimental results demonstrate that FAST has a high quality of detection for all forms of DDoS attacks.

In Arif et al. [75], the performance of DQQS was measured using three network metrics: throughputs, latency, and the chance of avoiding dangerous nodes. According to simulations, the suggested framework performs better in terms of throughput and latency than four cutting-edge routing algorithms: OSPF, L-L Routing, Sailfish Routing, and RL-Routing. For example, in an attack setting, the greatest throughput value of 14.5 Mbps was attained by the proposed DQQS model, outperforming OSPF at 8 Mbps, L-L at 8.2 Mbps, Sailfish at 9 Mbps, and RL at 9.5 Mbps. In a similar vein, this model outperformed the OSPF 88 ms, L-L 85 ms, Sailfish 72 ms, and RL 75 ms routing algorithms in terms of latency, with the lowest latency value of 52 ms. The experimental results indicate that the new DQQS model represents an important development in deep reinforcement learning, going over present deep learning methodologies in security and network performance metrics. This approach effectively tackles secure routing within the SDN-IoT framework, ensuring enhanced QoS and user experience.

A RL technique has been used in the research by Jin et al. [76] to reach Nash equilibrium policies for the two-player game between the attacker and the sensor. The problem of the remote security state estimation issue of CPSs with DoS assaults has been investigated. In addition, it is derived from two scenarios: reliable channel and unreliable channel, where the only possible causes of packet loss in reliable channel transmissions are DoS attacks and other causes may be the possible reason for loss of packets in unreliable channel transmissions. The paper also incorporates security state estimation into already-used RL techniques to assess how attacker and defense policies affect state estimation. The game between the attacker and the sensor is also described as a two-player zero-sum game, and Nash equilibrium tactics are researched to determine the best course of action. Additionally, the game takes into account the sensor's and the attacker's resource limitations. RL algorithms are made to allow sensors and attackers to adapt and learn policies in interactions, improving the ε-greedy strategy to strike a balance between exploration and exploitation.

Xu et al. [77] proposed a method for implementing route randomization at the packet level using programmable switches. The study employed robust network state awareness and developed random routing techniques with deep deterministic policy gradients to enhance the security and QoS for authorized network services. The proposed method utilizes in-band network telemetry to deliver precise, comprehensive, and instantaneous awareness of network conditions. Numerous trials indicate that the proposed strategy offers distinct advantages in security and usability against eavesdropping attacks relative to traditional route randomization defense strategies. The summary of the RL defense approaches for FA traffic is presented in Table 4.

Table 4 *The summary of RL for FA traffic*

Ref.	Model	Evaluation	Dataset	Advantage	Disadvantage
Zhang et al. [72]	A novel DRL framework	Time consumption	KDD99	It is capable of producing a satisfactory approximate outcome.	It is challenging for real-time systems to respond quickly enough to handle actual situations.
Veluchamy and Kathavarayan [73]	DARLH		UNSW-NB20, and Bot-IoT	The proposed model can defend against runtime DoS attack traffic with good results.	The model was not tested with massive traffic of DDoS attack
Li et al. [74]	FAST	F1-score and accuracy	Shenzhen taxicab dataset.	It adeptly picks characteristics in response to the dynamic IoV environment. It is efficient in detecting DDoS attacks in IoV with good accuracy	The model was not tested with massive traffic of DDoS attack
Arif et al. [75]	DQQS	Throughput, Latency, Probability, and accuracy	NSL-KDD	The proposed model optimizes the QoS And QoE within SDN-IoT environments. The model demonstrates superior performance in providing rapid and secure routing in SDN-IoT settings, effectively countering security threats at both the sensing and data layers.	The system is not tested with real-time traffic flows.
Jin et al. [76]	RL	Packet losses and running time	Generated	By rapidly converging to the Nash equilibrium policies of both sides, the model demonstrates the algorithm's availability and efficacy.	It can only detect limited types of flooding attacks.
Xu et al. [77]	Routing randomization based on deep reinforcement learning	Delay, Throughput,	Generated	The suggested DDPG-based approach proved to be dependable and effective in resolving the highly complex routing randomization challenge.	The system is not tested with real-time traffic flows. Also, the system is not tested with a large network.

4.5 Hybrid Learning

To perform well in detecting and classifying the FA, both DL and RL are combined to create deep reinforcement learning (DRL). It can now carry out a variety of intricate decision-making tasks that were before unsolvable for a machine. Furthermore, DRL has aided in the development of recent AI breakthroughs like OpenAI Five and AlphaGo. In fact, DRL has made a wide range of fascinating new research opportunities possible in fields including robotics, healthcare, smart grids, and finance.

In recent years, lots of efforts have been directed toward developing new algorithms combining deep learning and reinforcement learning tools in a new research field known as Deep reinforcement learning (DLR), such as Malialis and Kudenko, [78], mainly in the supervised Dong [80], Aamir et al. [81], Al-Shareeda et al. [82], and unsupervised domain Odumuyiwa and Alabi [83], Haldorai et al. [84], Tekleselassie [85], both to gain an advantage over classical machine learning, Deep learning algorithms and to control the complex systems more effectively.

A deep neural network whose objective function is the Bellman equation itself learns the policy in deep reinforcement learning. Starting with a random exploration of the space of potential actions, the network uses the

J. of Soft Computing and Data Mining Vol. 5 No. 2 (2024) p. 110-136

Bellman equation to iteratively reinforce its policy based on the reward received after each action. An ε-greedy policy is a typical method for moving from a merely random exploration to a conclusive reinforced policy. It selects the optimal provisional action with probability 1 − ε and a random action with probability 0 < ε- << 1. Moreover, a time-dependent slow decline of the parameter ε can yield a smooth transition. Fig. 9, which depicts the DRL architecture, visually represents the iterative process of the agent when interacting with the environment and collecting the information to build the knowledge base. Then, the policy π that the agent employs to interact with the surroundings is learned using a deep neural network. As seen in Fig. 8, the agent that learns and improves receives a reward and knowledge about the new state of the system.

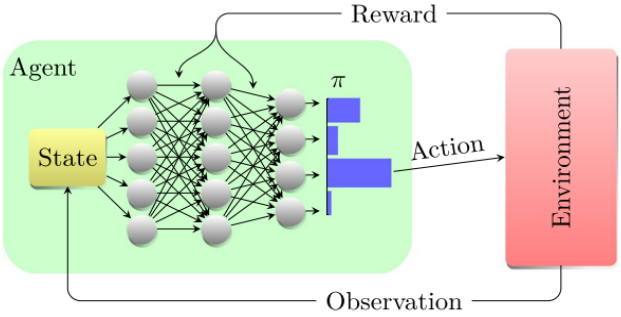


Fig. 8 *DLR architecture [78]*

Several studies have been well established by using DRL, in this section, the most effective studies have been presented. In the work of Malialis and Kudenko [77], The authors suggested DRL, a method that uses multi-agent router throttling to defend against DDoS attacks. They put forth a model that incorporates several agents engaged in reinforcement learning. Routers have these agents installed. The agents are trained to restrict or rate-limit traffic going to a victim server. It has been demonstrated to function effectively against DDoS attacks in small-scale network topologies. A statistical dataset with DDoS attack detection rate criteria was used to test the system. The suggested model had issues with scalability.

Malialis and Kudenko [78] introduced the Coordinated Team Learning (CTL) methodology. It involves installing numerous reinforcement learning agents on a group of routers. These agents pick up the ability to rate-limit or throttle traffic going to a victim server. Nevertheless, as each agent is limited to gathering local traffic facts, it becomes challenging to identify the best course of action. However, because discretizing the continuous action space induces the infamous combinatorial explosion and dimensionality curse, this approach is unable to fully utilize SDN and cannot be applied to a real large-scale network. A unique deep reinforcement learning-based strategy is put forth to address these issues and intelligently fight off DDoS attacks. In contrast to the previous study, the central deep reinforcement learning agent was positioned inside the SDN controller as opposed to being dispersed, allowing it to receive all original traffic data across the network and produce an optimal global policy to limit attack traffic. Using statistical data based on attack detection rate criteria, the CTL method tests and evaluates. Moreover, our method won't have the combinatorial explosion issue and won't significantly increase the overhead of SDN switches. Furthermore, since our method merely makes use of common OpenFlow APIs, it can be implemented on commercially available, off-the-shelf SDN switches without requiring additional deployment fees in a large-scale network.

More scalable than the solution suggested by Malialis and Kudenko [78], the Deep Deterministic Policy Gradient (DDPG) method was attempted to counteract DDoS attacks in the prior work of Qiu et al. [86]. Instead of being scattered among router sites, the DRL agents are positioned within the core Software Defined Network (SDN) in this method. The DRL agent that is suggested here controls the traffic that enters the server and keeps it from overflowing to avoid server overload. The DDPG method is used to train the mitigating agent, and each switch port's characteristics and flow statistics make up its state space. In this study, the writers have included eight features. Throttling traffic in accordance with the maximum bandwidth allotted to a particular host is an action performed by an agent. If the DDoS attack mitigating agent floods the server with excessive bandwidth, it will receive a negative reward. Additionally, the percentage of attack and benign traffic that reaches the server determines how much it is rewarded. The agent is always learning and has the ability to take command of the traffic going to the server. Thus, it succeeds in reducing the impact of DDoS attacks on the server. The suggested agent has the ability to counteract DDoS flooding assaults on several protocols, including TCP SYN, UDP, and ICMP.

A model called LSTM- Bayesian Attention (BA), developed by Li and Lu in [86], combines the LSTM and Bayes technique. This method uses network traffic to teach the LSTM the DDoS attack mode before predicting the likelihood of a DDoS attack. The proposed model has the ability to distinguish between normal and abnormal traffic with good performance. To test and evaluate the performance of the proposed model, the ISCX2012 dataset has been used. The obtained results show that the proposed system achieved good results when compared with

the related work that employed Deep Defense and Random Forest. The most accurate and high F1-score performer was LSTMBA. The generalization of LSTM-BA has also been confirmed by the authors, in addition to the aforementioned experiments. However, they examined how well LSTM-BA performs on data from the fifth day of the ISCX2012 dataset. The accuracy of the proposed model is only 0.16% better than the Deep Defense method currently in use.

Roopak et al. [87] developed the non-dominated sorting method (NSGA) approach for data preprocessing and normalization. In this study, the attack was classified using a CNN-LSTM combination. The CICIDS2017 dataset has been utilized in GPU experiments. The proposed approach had an F1-score value of 99.36% and a high accuracy of 99.03%. Additionally, authors have contrasted their approach with MLP, SVM, RF, Bayes, and other modern methodologies. Moreover, the obtained results indicated that the CNN-LSTM model outperformed previous research. The training time is reduced by an astonishing 11 times when contrasted with previous DL approaches. The CICIDS 2017 dataset is not utilized by the majority of the contemporary methodologies employed in this article. Consequently, the comparison appears to be unsuitable. The analysis of hybrid learning methods is presented in Table 2.6.

5. Datasets

This part includes a detailed presentation of datasets, as well as related and more recent types, which are essential for assessing the efficacy of suggested solutions.

5.1 CICIDS 2017 Dataset

The CICIDS2017 dataset was created by the University of New Brunswick (UNB) [89], in 2017, an emulated environment was used to create the CICDS2017 dataset [90]. This dataset includes network traffic in both a bidirectional flow-based and packet-based format. The authors of the CICIDS2017 dataset were Sharafaldin et al. [91]. It uses normal routine operations as well as attacks, including DoS, Heartbleed, Brute Force SSH, Web Attack, Botnet, Infiltration, DDoS, and Brute Force FTP [89]. The CICFlowMeter tool was used on the produced network traffic to extract more than 80 features for each flow. Whereas, the CICIDS 2017 dataset generated the abstract behavior for more than 20 subscribers based on email; Hypertext Transfer Protocol Secure (HTTP), Secure Shell (SSH), Secure File Transfer Protocol (SFTP), and HTTPS protocols. There are more than 500,000 malicious records and more than two million benign request.

5.2 CSE-CIC-IDS 2018 Dataset

The University of New Brunswick (UNB) is responsible for the development of the Communications Security Establishment and the Canadian Institute for Cybersecurity dataset [92]. From Wednesday (14-02-2018) to Friday (02-03-2018), UNB implemented this dataset by collecting data for a period of ten days. This dataset, which was constructed on a substantial network, contains seven distinct attack scenarios, including Heartbleed, Botnet, Brute force, DoS, Web attacks, DDoS, and internal network infiltration. The CIC Flow Meter utility [88] extracted eighty features from the network traffic that was generated.

5.3 CICIDS2019 Dataset

A common benchmark dataset for assessing IDSs is CICIDS 2019. The Canadian Institute for Cybersecurity (CIC) dataset was developed by the University of New Brunswick (UNB) [93]. In 2019, the most recent and secure DDoS attacks that replicate actual real-world data (PCAPs) are incorporated. It also includes designated flows that are based on time stamps, source and destination IP addresses, source and destination ports, protocols, and attack vectors, as derived from the network traffic analysis conducted using CICFlowMeter-V3 (CSV files).

5.4 CIC-Bell-DNS-EXF-2021 Dataset

The University of New Brunswick's Canadian Institute for Cybersecurity produced the CICIDS2019 dataset, which is a dataset of network traffic [94]. It was produced in order to supply network traffic information for network intrusion detection system (NIDS) assessment. This massive dataset of 270.8 MB DNS traffic was obtained by the exfiltration of several file kinds, varying in size from tiny to large. Using our developed feature extractor, 30 features were extracted from the DNS packets to construct a final structured dataset that included 323,698 heavy attack samples, 53,978 light attack samples, and 641,642 unique benign samples [92].

5.5 UNSWNB15 Dataset

The UNSW-NB15 Dataset 2021 Dataset was created by Intelligent Security Group (ISG), Canberra, Australia in 2021 [95]. It is a standard benchmark dataset for evaluating IDSs. It was created in the Australian Centre for Cyber

Security's (ACCS) Cyber Range Lab. This dataset was produced using the IXIA Perfect Storm, argus, bro-IDS, and tcpdump tools. The IXIA Perfect Storm program was utilized to generate a mix of typical and unusual network traffic. Fuzzers, reconnaissance, exploits, backdoors, generic, shellcode, denial-of-service, worms, and analysis assaults are the nine varieties of attacks that the IXIA tool may produce. Using the tcpdump utility, the packets representing the network traffic were captured. The dataset's simulation time for capturing 100 GBs was 31 hours, with 16 hours on January 22 and 15 hours on February 17 making up the total. By utilizing the Argus and bro-IDS tools, the trustworthy features were extracted from the pcap data. A total of 49 features are available. Also, twelve algorithms were developed in C# to examine the connection packet flow. A total of 2,540,044 million records are present, with 2,218,761 being benign and 321,283 being malevolent.

5.6 CICIoMT 2024 Dataset

A publicly accessible dataset for Internet of Things (IoT) security research is the CICIoMT2024 dataset. It includes statistics on network traffic that has been gathered from different IoT networks and devices. A topology of 105 IoT devices is used to carry out 33 assaults. The seven categories into which these assaults are divided are DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, and Mirai. Furthermore, every assault is carried out by malevolent IoT devices that are directed at other IoT devices [96]. This dataset allows IoT professionals to create novel security analytics solutions by containing multiple attacks that are not available in other IoT datasets. Additionally, the data are accessible in a variety of formats, enabling researchers to create new characteristics or utilize features that were taken from our study.

However, all the above-mentioned datasets have been widely used in network security research, particularly for the evaluation and development of the performance of the protection systems models and techniques. It provides a comprehensive and realistic dataset for researchers to test their solutions on a variety of modern network attack scenarios. Table 5 shows the summary of the above-mentioned datasets.

Table 5 *Dataset analysis table*

No.	Ref.	Dataset name	Protocol	Layer
1	UNB [75]	CICIDS2017	SSH, FTP, and HTTP	Application and Transport
2	CIC-UNB [79]	CSE-CIC-IDS 2018	SSH, FTP, IMAP, POP3, SMTP, and HTTP	Application and Transport
3	UNB [80]	CICIDS2019	TCP/UDP	Transport
4	UNB [81]	CIC-Bell-DNS-EXF-2021	DNS	Application
5	ISG [82]	UNSWNB15 2021	TCP	Transport
7	UNB [84]	CICIoMT2024	ISMP, TCP/UDP	Application and Transport

6. Conclusion

A lot of changes have been made to smart cities in an effort to radically change people's lives. However, despite the fact that smart cities offer enormous convenience and substantially raise people's quality of life, there are still unresolved cyber security issues, like aggressive cyberattacks and data breaches. Because smart city cyberspace is growing at a faster rate than current cyber security breakthroughs, the defense model's effective design is essential for protecting it. The current paper goes into great detail on smart city architecture and the advanced attack vectors that could be used against it. The study also offers a summary of the ideas of cyber security, learning-based defense strategies, and smart cities and looks at the literature that is currently available on IoT security in smart cities. Specifically, a number of learning method models were briefly reviewed, including Reinforcement Learning, Semi-Supervised Learning, Instance Supervised Learning, and Hybrid Learning methods. The paper also provides examples of the testing datasets that were used to assess and test the effectiveness of the suggested defense strategies. The investigation developments in ML and DL for threat detection, blockchain technology for security, and zero-trust architecture are recommended for future work.

Acknowledgment

The authors would like to thank the School of Computing, Universiti Teknologi Malaysia, for supporting this work

Conflict of Interest

The authors declare that they have no conflicts of interest related to this work that need to be addressed.

Author Contribution

The authors assert their contribution to the manuscript as follows: ***Study design and conception:*** *Bashar A. Khalaf and Siti H. Othman.* ***Results analysis and interpretation:*** *Shukor A. Razak Author.* ***First draft of paper preparation:*** *Bashar Ahmed Khalaf.* ***Manuscript previewed:*** *Alexandros K. Author.*

References

[1] Alexandro, R., & Basrowi, B. (2024). Measuring the effectiveness of smart digital organizations on digital technology adoption: An empirical study of educational organizations in Indonesia. International Journal of Data and Network Science, 8(1), 139-150.

[2] Khalaf, B. A., Othman, S. H., Razak, S. A., & Konios, A. (2024). A Hybrid Deep Learning Model for Securing Smart City Networks Against Flooding Attack. *Journal of Cybersecurity & Information Management*, *14*(2).

[3] Lai, C. S., Jia, Y., Dong, Z., Wang, D., Tao, Y., Lai, Q. H., ... & Lai, L. L. (2020). A review of technical standards for smart cities. Clean Technologies, 2(3), 290-310.

[4] Arshad, S., Azam, M. A., Ahmed, S. H., & Loo, J. (2017, July). Towards information-centric networking (ICN) naming for Internet of Things (IoT) the case of smart campus. In Proceedings of the International Conference on Future Networks and Distributed Systems (pp. 1-6).

[5] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3), e3677.

[6] Toh, C. K. (2020). Security for smart cities. IET Smart Cities, 2(2), 95-104.

[7] Ali, S., & Li, Y. (2019). Learning multilevel auto-encoders for DDoS attack detection in smart grid network. IEEE Access, 7, 108647-108659.

[8] Rizwan, P., Suresh, K., & Babu, M. R. (2016, October). Real-time smart traffic management system for smart cities by using Internet of Things and big data. In 2016 international conference on emerging technological trends (ICETT) (pp. 1-7). IEEE.

[9] Rathore, M. M., Paul, A., Ahmad, A., Chilamkurti, N., Hong, W. H., & Seo, H. (2018). Real-time secure communication for Smart City in high-speed Big Data environment. Future Generation Computer Systems, 83, 638-652.

[10] Burhan, M., Alam, H., Arsalan, A., Rehman, R. A., Anwar, M., Faheem, M., & Ashraf, M. W. (2023). A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: layered architecture, real-time security issues, and solutions. IEEE Access.

[11] Das, R., & Inuwa, M. M. (2023). A review on fog computing: issues, characteristics, challenges, and potential applications. Telematics and Informatics Reports, 100049.

[12] Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 215, 108975.

[13] Khalil, U., Malik, O. A., Uddin, M., & Chen, C. L. (2022). A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. Sensors, 22(14), 5168.

[14] Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems, 73(1), 3-25. Majeed, U., Khan, L. U., Yaqoob, I., Kazmi, S. A., Salah, K., & Hong, C. S. (2021). Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications, 181, 103007.

[15] Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable cities and society, 38, 697-713.

[16] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business horizons, 58(4), 431-440.

[17] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377.

[18] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691-51713.

[19] Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H., & Zhang, W. (2022). CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities. Microprocessors and Microsystems, 90, 104504.

[20] Fard, S. M. H., Karimipour, H., Dehghantanha, A., Jahromi, A. N., & Srivastava, G. (2020). Ensemble sparse representation-based cyber threat hunting for security of smart cities. Computers & Electrical Engineering, 88, 106825.

[21] Din, I. U., Guizani, M., Rodrigues, J. J., Hassan, S., & Korotaev, V. V. (2019). Machine learning in the Internet of Things: Designed techniques for smart cities. Future Generation Computer Systems, 100, 826-843.

[22] Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials, 21(3), 2794-2830.
[23] Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable cities and society, 39, 499-507.
[24] Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In Smart Cities and Innovative Urban Technologies (pp. 47-65). Routledge.
[25] Schiavone, F., Appio, F. P., Mora, L., & Risitano, M. (2020). The strategic, organizational, and entrepreneurial evolution of smart cities. International Entrepreneurship and Management Journal, 16(4), 1155-1165.
[26] Ali, S., & Li, Y. (2019). Learning multilevel auto-encoders for DDoS attack detection in smart grid network. IEEE Access, 7, 108647-108659.
[27] Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H., & Zhang, W. (2022). CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities. Microprocessors and Microsystems, 90, 104504.
[28] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 24(2), 393-414.
[29] Hamidouche, R., Aliouat, Z., Ari, A. A. A., & Gueroui, M. (2019). An efficient clustering strategy avoiding buffer overflow in IoT sensors: A bio-inspired based approach. IEEE Access, 7, 156733-156751.
[30] Ullah, A., Anwar, S. M., Li, J., Nadeem, L., Mahmood, T., Rehman, A., & Saba, T. (2024). Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex & Intelligent Systems, 10(1), 1607-1637.
[31] Shukla, P. (2017, September). ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In 2017 Intelligent Systems Conference (IntelliSys) (pp. 234-240). IEEE.
[32] He, J., Tan, Y., Guo, W., & Xian, M. (2020, August). A small sample DDoS attack detection method based on deep transfer learning. In 2020 International Conference on Computer Communication and Network Security (CCNS) (pp. 47-50). IEEE.
[33] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., Mahmoud, M. A., Al-Rimy, B. A. S., ... & Marks, A. (2021). An adaptive protection of flooding attacks model for complex network environments. Security and Communication Networks, 2021, 1-17.
[34] Xue, L., Ma, X., Luo, X., Chan, E. W., Miu, T. T., & Gu, G. (2018). Linkscope: Toward detecting target link flooding attacks. IEEE Transactions on Information Forensics and Security, 13(10), 2423-2438.
[35] Aydeger, A., Manshaei, M. H., Rahman, M. A., & Akkaya, K. (2021). Strategic defense against stealthy link flooding attacks: a signaling game approach. IEEE Transactions on Network Science and Engineering, 8(1), 751-764.
[36] Rasool, R. U., Ashraf, U., Ahmed, K., Wang, H., Rafique, W., & Anwar, Z. (2019). Cyberpulse: a machine learning based link flooding attack mitigation system for softlearning-based link flooding attack mitigation system for software-definedg, W. K., Wang, C. X., Tsai, S. C., & Lin, Y. B. (2021). Efficient Detection of Link-Flooding Attacks with Deep Learning. Sustainability, 13(22), 12514.
[37] Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 105124.
[38] Goodfellow I, Bengio Y, Courville A (2016) Deep learning. MIT Press, Cambridge Google services resume after massive gmail, youtube outage. https:// www.livemint.com/technology/apps/google-services-youtubegmail-google-drive-face-outage-11607947475759.html. 18 Apr 2021.
[39] Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, 169, 102767.
[40] Yuvaraj, N., Raja, R. A., Kousik, N. V., Johri, P., & Divan, M. J. (2020). Analysis on the prediction of central line-associated bloodstream infections (CLABSI) using deep neural network classification. In Computational Intelligence and Its Applications in Healthcare (pp. 229-244). Academic Press.
[41] Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J. M., & Kim, D. S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. Computer Networks, 188, 107871.
[42] Virupakshar, K. B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D. G. (2020). Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Computer Science, 167, 2297-2307.
[43] Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). Deepdetect: detection of distributed denial of service attacks using deep learning. The Computer Journal, 63(7), 983-994.
[44] Muraleedharan, N., & Janet, B. (2021). A deep learning based HTTP slow DoS classification approach using flow data. ICT Express, 7(2), 210-214.
[45] Sbai, O., & El boukhari, M. (2020, September). Data flooding intrusion detection system for manets using deep learning approach. In Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications (pp. 1-5).

[46] Hasan, M. Z., Hasan, K. Z., & Sattar, A. (2018). Burst header packet flood detection in optical burst switching network using deep learning model. Procedia computer science, 143, 970-977.
[47] Amma, N. G. B., & Subramanian, S. (2018, October). Vcdeepfl: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks. In TENCON 2018-2018 IEEE Region 10 Conference (pp. 0640-0645). IEEE.
[48] Shaaban, A. R., Abd-Elwanis, E., & Hussein, M. (2019, December). DDoS attack detection and classification via Convolutional Neural Network (CNN). In 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS) (pp. 233-238). IEEE.
[49] Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K. K. R., & Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. Ieee Access, 8, 53972-53983.
[50] Jacob, S., Qiao, Y., & Lee, B. (2021). Detecting Cyber Security Attacks against a Microservices Application using Distributed Tracing. In ICISSP (pp. 588-595).
[51] Yu, B., Yin, H., & Zhu, Z. (2017). Spatio-temporal graph convolutional networks: A deep learning framework for traffic forecasting. arXiv preprint arXiv:1709.04875.
[52] Chen, J., Yang, Y. T., Hu, K. K., Zheng, H. B., & Wang, Z. (2019, February). DAD-MCNN: DDoS attack detection via multi-channel CNN. In Proceedings of the 2019 11th International Conference on Machine Learning and Computing (pp. 484-488).
[53] Nisha, S. S., Sathik, M. M., & Meeral, M. N. (2021). Application, algorithm, tools directly related to deep learning. In Handbook of Deep Learning in Biomedical Engineering (pp. 61-84). Academic Press.
[54] Li, Y., Yu, R., Shahabi, C., & Liu, Y. (2017). Diffusion convolutional recurrent neural network: Data-driven traffic forecasting. arXiv preprint arXiv:1707.01926.
[55] Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X., & Gong, L. (2018). Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. International Journal of Communication Systems, 31(5), e3497.
[56] Liang, X., & Znati, T. (2019, December). A long short-term memory enabled framework for DDoS detection. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.
[57] Liu, G., Quan, W., Cheng, N., Zhang, H., & Yu, S. (2019). Efficient DDoS attacks mitigation for stateful forwarding in the Internet of Things. Journal of Network and Computer Applications, 130, 1-13.
[58] Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Philip, S. Y. (2020). A comprehensive survey on graph neural networks. IEEE transactions on neural networks and learning systems, 32(1), 4-24.
[59] Shurman, M. M., Khrais, R. M., & Yateem, A. A. (2020). DoS and DDoS attack detection using deep learning and IDS. Int. Arab J. Inf. Technol., 17(4A), 655-661.
[60] Assis, M. V., Carvalho, L. F., Lloret, J., & Proença Jr, M. L. (2021). A GRU deep learning system against attacks in software defined networks. Journal of Network and Computer Applications, 177, 102942.
[61] Rasmus, A., Berglund, M., Honkala, M., Valpola, H., & Raiko, T. (2015). Semi-supervised learning with ladder networks. Advances in neural information processing systems, 28.
[62] Sanchez-Lengeling, B., Reif, E., Pearce, A., & Wiltschko, A. B. (2021). A gentle introduction to graph neural networks. Distill, 6(9), e33.
[63] Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 105124.
[64] Catak, F. O., & Mustacoglu, A. F. (2019). Distributed denial of service attack detection using autoencoder and deep neural networks. Journal of Intelligent & Fuzzy Systems, 37(3), 3969-3979.
[65] Yang, K., Zhang, J., Xu, Y., & Chao, J. (2020, April). Ddos attacks detection with autoencoder. In NOMS 2020-2020 IEEE/IFIP network operations and management symposium (pp. 1-9). IEEE.
[66] Kasim, Ö. (2020). An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. Computer Networks, 180, 107390.
[67] Bhardwaj, A., Mangat, V., & Vig, R. (2020). Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. IEEE Access, 8, 181916-181929.
[68] Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems, 79, 103278.
[69] Hernandez-Leal, P., Kartal, B., & Taylor, M. E. (2019). A survey and critique of multiagent deep reinforcement learning. Autonomous Agents and Multi-Agent Systems, 33(6), 750-797.
[70] Zhang, H., Hao, J., & Li, X. (2020). A method for deploying distributed denial of service attack defense strategies on edge servers using reinforcement learning. IEEE Access, 8, 78482-78491.
[71] Feng, Y., Zhang, W., Yin, S., Tang, H., Xiang, Y., & Zhang, Y. (2023). A Collaborative Stealthy DDoS Detection Method based on Reinforcement Learning at the Edge of the Internet of Things. IEEE Internet of Things Journal.
[72] Veluchamy, S., & Kathavarayan, R. S. (2022). Deep reinforcement learning for building honeypots against runtime DoS attack. International Journal of Intelligent Systems, 37(7), 3981-4007.

[73] Li, Z., Kong, Y., Wang, C., & Jiang, C. (2021). DDoS mitigation based on space-time flow regularities in IoV: A feature adaption reinforcement learning approach. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2262-2278.
[74] Arif, F., Khan, N. A., Iqbal, J., Karim, F. K., Innab, N., & Mostafa, S. M. (2024). DQQS: Deep Reinforcement Learning based Technique for Enhancing Security and Performance in SDN-IoT Environments. IEEE Access.
[75] Jin, Z., Zhang, S., Hu, Y., Zhang, Y., & Sun, C. (2022, July). Security state estimation for cyber-physical systems against DoS attacks via reinforcement learning and game theory. In Actuators (Vol. 11, No. 7, p. 192). MDPI.
[76] Xu, X., Hu, H., Liu, Y., Tan, J., Zhang, H., & Song, H. (2022). Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack. Digital Communications and Networks.
[77] Malialis, K., & Kudenko, D. (2013, July). Multiagent router throttling: Decentralized coordinated response against DDoS attacks. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 27, No. 2, pp. 1551-1556).
[78] Malialis, K., & Kudenko, D. (2015). Distributed response to network intrusions using multiagent reinforcement learning. Engineering Applications of Artificial Intelligence, 41, 270-284.
[79] Dong, S., Xia, Y., & Peng, T. (2021). Network abnormal traffic detection model based on semi-supervised deep reinforcement learning. IEEE Transactions on Network and Service Management, 18(4), 4197-4212.
[80] Aamir, M., & Zaidi, S. M. A. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. Journal of King Saud University-Computer and Information Sciences, 33(4), 436-446.
[81] Al-Shareeda, M. A., Manickam, S., & Ali, M. (2023). DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. Bulletin of Electrical Engineering and Informatics, 12(2), 930-939.
[82] Odumuyiwa, V., & Alabi, R. (2021). DDOS detection on internet of things using unsupervised algorithms. Journal of Cyber Security and Mobility, 569-592.
[83] Haldorai, A., Ramu, A., & Suriya, M. (2020). Organization internet of things (IoTs): Supervised, unsupervised, and reinforcement learning. In Business Intelligence for Enterprise Internet of Things (pp. 27-53). Cham: Springer International Publishing.
[84] Tekleselassie, H. (2021). DDoS detection on Internet of Things using unsupervised algorithms. In E3S Web of Conferences (Vol. 297, p. 01005). EDP Sciences.
[85] Qiu, C., Hu, Y., Chen, Y., & Zeng, B. (2019). Deep deterministic policy gradient (DDPG)-based energy harvesting wireless communications. IEEE Internet of Things Journal, 6(5), 8577-8588.
[86] Li, Y., & Lu, Y. (2019, September). LSTM-BA: DDoS detection approach combining LSTM and Bayes. In 2019 Seventh International Conference on Advanced Cloud and Big Data (CBD) (pp. 180-185). IEEE.
[87] Roopak, M., Tian, G. Y., & Chambers, J. (2020, January). An intrusion detection system against DDoS attacks in IoT networks. In 2020 10th annual computing and communication workshop and conference (CCWC) (pp. 0562-0567). IEEE.
[88] University of New Brunswick (UNB), CIC-IDS 2017 (2017), available at https://www.unb.ca/cic/datasets/ids-2017.html. Accessed on 2017.
[89] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147-167.
[90] Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019, October). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.
[91] University of New Brunswick (UNB), CSE-CIC-IDS, 2018, available at https://www.unb.ca/cic/datasets/ids-2018.html, Accessed on 2018.
[92] University of New Brunswick (UNB), CIC-IDS2019 (2019), available on https://www.unb.ca/cic/datasets/ddos-2019.html. Accessed in 2019.
[93] University of New Brunswick (UNB), CIC-Bell-DNS-EXF-2021 dataset, available at https://www.unb.ca/cic/datasets/dns-exf-2021.html. Accessed in 2021.
[94] Intelligent Security Group (ISG), UNSWNB15 Dataset 2021, available on https://research.unsw.edu.au/projects/unsw-nb15-dataset. Accessed on 2021.