Critical Infrastructures: Presentation, cyberattacks and protection Mechanisms – A Survey

Semou NDIAYE[1*], *Idy DIOP*[1], Saïdou Talla [1]

[1] IT Engineering Department Polytechnic School, Cheikh Anta Diop University Dakar, Senegal

Abstract. In recent years, the world has seen great achievements in the development of the infrastructure needed for information and communication technologies, and widespread and growing access to high-speed Internet. Today, governments, businesses, civil society and individuals across the planet are increasingly connected to this vast network. However, the significant growth of the internet has also led to new cybersecurity challenges for the global community. The more interconnected our societies become, the more vulnerable our critical infrastructures are to cyber threats. More and more critical infrastructures are falling victim to DDoS or malware attacks, and the trend is not decreasing.
It is therefore urgent to find defence methods against these attacks
In this article, we present the state of the art in attack methods against critical infrastructures, as well as the defence methods implemented against these attacks.

Keywords—critical infrastructures, cyberattacks, DDoS, malware, defence

1 Introduction

Critical infrastructures are essential to the proper functioning of a State, a society or its economy. They include many different types of activity, such as the electricity grid, the oil and gas sector, telecommunications, public health, water supply systems, air traffic control systems, financial services, etc. These infrastructures are of the utmost importance, and relatively minor failures can have a significant impact on a large number of people.
Over the past two decades, the Internet has grown exponentially and has become part of our daily lives. Our national critical infrastructure networks are increasingly connected to the Internet to provide benefits such as: cost reduction, where large systems can be managed remotely over the public network; increased capacity - by providing sufficient computing resources for infrastructure hardware; improved efficiency and speed, etc. [1]. As a result, critical infrastructures are becoming increasingly dependent on digital systems. Not surprisingly, new cyber threats are emerging, and nations and organizations are facing

* semoundiaye88@gmail.com

vulnerabilities on new fronts that are likely to be amplified by the connectivity of these systems [2].
As a result, infrastructures the world over are facing an upsurge in cyber-attacks. These attacks are most often perpetrated by hacktivists, cyber-criminals or cyber-terrorists, but also by one state against another. The aim of many cyber-attacks on critical infrastructures is to take control of them for the purposes of terrorist attacks, to extract secret information or personal data, sabotage, and more.
In this article, we take a survey on critical infrastructures.
Firstly, we will present the critical infrastructures. Secondly, we will look the attack methods used in our critical infrastructure systems. Thirdly and lastly, we will look at existing defence methods against these attacks.

2 Critical infrastructures

2.1 Clarification of concepts

The terms used to describe critical infrastructures are numerous and varied.
In [3], the authors considered a critical infrastructure to be a set of organizations, facilities, equipment, logical and physical assets, which is of vital or critical importance to the functioning of an economy in particular or human society in general, and whose failure, stop or degradation can have a potentially dramatic impact on the economic and social well-being of a nation.
According to Zhang & al [4], critical infrastructures are generally understood to include those facilities and services that are vital to the basic functioning of society and whose disruption or destruction could significantly impair the functioning of society.
According to ECOWAS [5], critical infrastructure is a public or private process whose destruction, disruption, illegitimate operation or disruption for a defined period of time could result in the loss of human life, significant losses to the economy or considerable damage to the reputation of the State or its symbols of governance. In this definition, infrastructure includes the networks and systems and the physical or digital data required to provide the service. This expression may refer to a system or process whose operation is critical within the organization (ECOWAS).
In its directive 2008/114/EC [6], the Council of Europe gives the following definition: "critical infrastructure is a point, system or part thereof located in the Member States which is essential for maintaining the vital functions of society, the health, safety, security and economic or social well-being of citizens, and whose disruption or destruction would have a significant impact in a Member State because of the failure of those functions".
These definitions are all representative of critical infrastructures.
However, the notion of critical infrastructure is difficult to pin down and to define in an unequivocal, permanent and universal way.
Being relative in nature, the critical or non-critical nature of an infrastructure can change depending on what it represents in the economic, social and security life of a nation, or even its symbolic value, once it is the target of a threat or attack. So, for example, the Bardo museum in Tunis, the seaside resort of Sharm-el-Sheikh in Egypt, or the Radisson Blu hotel in Bamako, were not intended to be classified as “vital infrastructures”. However, the symbolism they represented and the dazzling nature of the terrorist acts carried out there in 2015 have had a catastrophic impact on the growth of terrorism in the countries affected, and hence on national life and security [7]. This raises the question of whether luxury hotels with a well-established reputation can be classified as "vital infrastructure" in certain countries.

Indeed, no one needs to demonstrate that the "slump" in the tourism sector necessarily leads to an increase in unemployment, with all the political and social consequences that this entails. What's more, in some countries (Burkina Faso, Chad, Niger, ...) this sector may be important but not "vital", while in others (Tunisia, Egypt, Senegal, Gambia, ...) it is an activity at the heart of national life.
Furthermore, in the USA, the protection of the presidential aircraft Air Force One becomes a matter of national security when the President is on board. When this happens, the aircraft is "of vital importance", which is certainly not the case when it is in the hangar without its designated passenger. This same qualification applies to all countries in the world that are concerned to protect their institutions.
Nevertheless, it can be said that an infrastructure becomes "critical", "vital" or "sensitive", depending on the terminology used by each country, when its total or partial destruction would have serious consequences for the life of the population, the State or its institutions, and for public life. A critical, vital, sensitive or essential infrastructure is therefore by its very nature essential to the life of the population, the country's economy, the normal functioning of society and the stability of its institutions.

2.2 Identification

The process of identifying critical infrastructures is based on several criteria, depending on the sector and also the geopolitical zone. It is up to each government to define the critical nature of these infrastructures. Each country adopts its own definition and terminology according to its own assessment criteria and national and security policy priorities. The following table shows the infrastructures and sectors that can be classified as vital.

Table 1. Infrastructures and services that may be classified as critical

Sectors	Infrastructures and services
1. State activities	- Public safety - Internal security - Legal services - National defence - Public finance - Parliament - Electoral processes - Electronic administration
2. Energy	- Electricity generation, transmission and distribution - Production, transport, refining, storage and distribution of petroleum products - Production, transport, treatment, storage and distribution of gas - Nuclear facilities
3. Transport	- Air, road, rail, sea and river transport - Air traffic control - Management of airport and port platforms (including security systems)

	- Road and rail infrastructure management
4. Logistics	- Management of logistics platforms
5. Finance	- Distribution of minimum social benefits (safety net/financial assistance/social incentives) - Collection and cash management for social security bodies - Banking transactions - Financial services and credit clearing - Financial market infrastructures
6. Health	- Unique healthcare capabilities or procedures (in facilities or via telemedicine) - Pharmaceutical distribution - Research laboratories - Medical records databases
7.Water and Sewerage	- Production, transport, storage and distribution of drinking water (piped or bottled) - Wastewater collection and management systems
8. Electronic communications	Production, transport, storage and distribution of drinking water (piped or bottled) Wastewater collection and management systems National Internet network and interconnection to the regional and global Internet (submarine and terrestrial cables, cable landing points, Internet exchange points, etc.). Internet domain name management (DNS) Internet access Telecommunications services (telephony, ...) Datacenters, including national datacenters
9. Information	- radio and television stations
10. Power supply	- Supply, storage and distribution of the main foodstuffs
11. Industry	- Key industries for the country
12. Miscellaneous	- Infrastructures likely to cause serious damage to the population in the event of acci-dental or malicious destruction (e.g. dams)

2.3 Interdependence

A critical infrastructure may be autonomous or part of a complex, interdependent system (Fig.1). So, for example, a large-scale interruption or sabotage of an electrical installation will have consequences for the water supply, telecommunications, transport, and so on.
The interconnectedness of the various sectors managing critical infrastructures (such as energy, transport and finance) means that a cyber-attack on one sector could have cascading effects on other sectors, amplifying its overall impact.

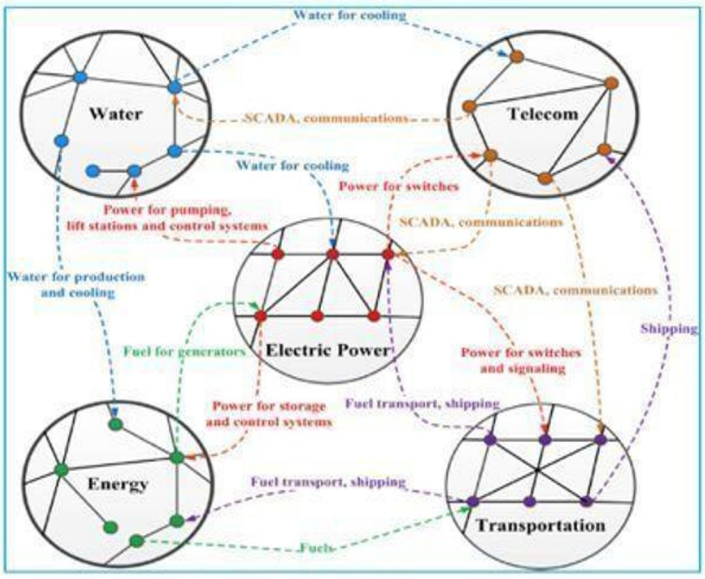

Fig. 1. A case of critical infrastructures interdependence

3 Attacks methods

Critical infrastructures can be compromised in many ways, either maliciously or accidentally, or simply by the failure of a computer system.
While organizations must take all these risks into account, malicious Internet attacks are potentially the most damaging of all [8]. These attacks can be carried out in many different ways. However, DDoS and malware attacks are the most widespread

3.1 DoS/DDoS attacks

A Denial of Service (DoS) attack is a type of attack aimed at making an organization's services or resources unavailable for an indefinite period of time. In most cases, these attacks are aimed at a company's servers, so that they cannot be used or accessed [9]. When a connection is requested, the server is put on hold and blocks part of its resources for the new connection.
The aim is to send more connection requests than it can handle in a given time. The server will no longer be able to meet the needs of real customers.
A DDoS (Distributed Denial of Service) attack is similar to a DoS attack, but is carried out from multiple machines. Many hackers use botnets (or zombie computers) to execute DDoS attacks. A botnet is a way for a single person (a hacker, for example) to control thousands of devices at once. The following diagram illustrates a DDoS attack.

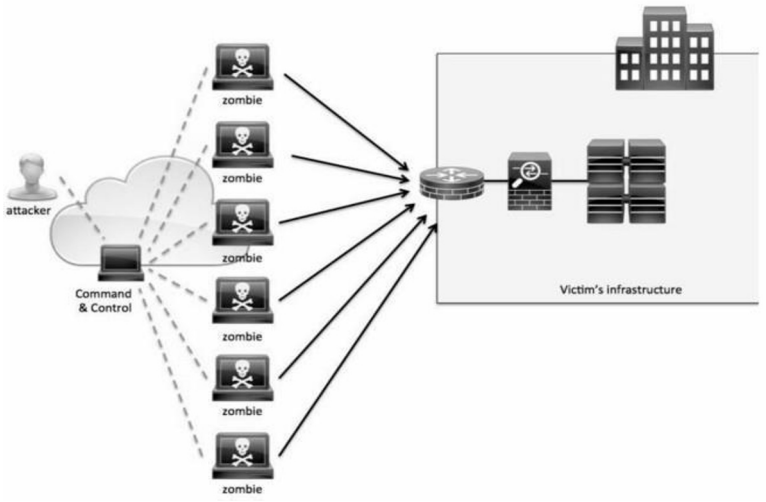

Fig. 2. DDoS attack

Many critical infrastructures are targets of large-scale DDoS attacks. Take, for example, the DDoS attack against Liberia in 2016, which targeted over half a million security cameras worldwide attempting to connect to a handful of servers used by Lonestar Cell MTN, a local mobile operator. As a result, Lonestar's network was overwhelmed and Internet access for its 1.5 million customers slowed and then stopped [10].
In 2017, DDoS attacks against Amazon and Google were reported [11][12]. The attack against Google lasted over a six-month campaign, reaching a peak of 2.5Tbit/s.

3.2 Malware Attacks

Malware is a program or part of a program designed to disrupt, alter or destroy all or part of the software elements essential to the proper operation of a computer system [9]. This broad definition encompasses a wide range of programs with very different functions and features (viruses, worms, ransomware, spyware, logic bombs, etc.), all of which share the common

aim of carrying out a number of actions that are generally unwanted by the user: remote control, espionage, data theft, etc.

One of the biggest malware attacks on critical infrastructures is the Stuxnet worm attack on Iran's nuclear facilities. The Stuxnet worm first appeared in the summer of 2010 [13]. It is a 500-kilobyte worm that has infiltrated numerous computer systems. The virus works in three stages. First, it scans and targets Windows networks and computer systems. Having infiltrated these machines, the worm begins to reproduce itself continuously. Next, the machine infiltrates the Windows-based Siemens Step7 software. This Siemens software system was and continues to be widespread in industrial computer networks, such as nuclear enrichment facilities. Finally, by compromising the Step7 software, the worm gains access to the logic controllers of the industrial program [14]. As a result, more than fifteen Iranian facilities have been attacked and infiltrated by the Stuxnet worm. The attack is thought to have been initiated by a random worker's USB key. One of the industrial facilities affected was the Natanz nuclear facility [13]. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of centrifuges enriching uranium were breaking down. The cause of these failures was unknown at the time. Later, Iranian technicians hired computer security specialists in Belarus to examine their computer systems. This security firm eventually discovered several malicious files on the Iranian computer systems. It later revealed that these malicious files were the Stuxnet worm. Although Iran has not released specific details about the effects of the attack, it is estimated that the Stuxnet worm destroyed 984 centrifuges enriching uranium [15].

In 2015, a piece of malware (a Trojan) called “Duuzer” was detected in South Korean manufacturing companies. The malware was used to steal valuable data and demand ransom from electronic manufacturing companies that were apparently headquartered in the same country [16].

In May 2016, the victim of multiple ransomware threats was a hospital located in Kansas. A piece of software was identified as the “Samsam” malware. Although the ransom was sent by the hospital, the cyber actors did not return full access to the data [17]. The authors of the attack demanded another sum to be paid, which led the hospital to refuse the new payment. The report did not clearly identify whether the hospital resolved the attack with mitigating measures or received the decryption key [18]. Another attack against the healthcare sector took place on March 29, 2016. The Washington Post reported that more than 250 outpatient centers in 10 hospitals were forced to shut down their computer systems. Important data such as patient histories, prescriptions, etc. disappeared after the attack. As a result, patients were redirected to other medical centers and rescheduled appointments [19]. Similarly, another threat emerged in 2016, where attackers encrypted the emails and patient diaries of a California-based hospital. The initial ransom was $3 million, but after negotiations with the players, this was changed to $17,000 [20].

In June 2017, the cyber threat Petya hit many computers around the world, causing systems to become infected by encrypting data and demanding a ransom. When numerous investigations were carried out, it became apparent that it was comparatively similar to the “WannaCry” ransomware attack the world had previously taken note of. The Petya ransomware exploited Windows vulnerabilities in certain protocols (SMB, Server Message Block) as well as other exploits such as collecting credentials and running remote utilities. The attack was propagated across networks by overwriting the Master Boot Record (MBR). Focusing on the recent WannaCry spread that took place in May 2017, it was noted that many victims' operating systems were not protected against this vulnerability. With regard to the Petya ransomware attack, it can be noted that, despite the recent incident of the WannaCry attack, there are still 3 a number of systems with the same unpatched vulnerabilities [17].

On the African continent, we can mention the attack against City Power, a company responsible for supplying power to the city of Johannesburg, which occurred in 2019. In fact,

the attack was caused by malware that encrypted all the company's application and network databases, preventing it from operating [21].

4 Defence methods

4.1 Defence against DDoS attacks

DDoS attacks have evolved rapidly over time and have become highly sophisticated. They seriously affect an organization's IT, financial and infrastructure resources. The number of DDoS attacks has increased exponentially over the years, not even sparing major cloud service providers such as Microsoft and Amazon EC2 [10]. The seriousness of the DDoS problem and the increasing frequency, sophistication and power of attacks have led to the proposal of numerous defence mechanisms.

Thus, in [22] the authors proposed a proactive method for estimating the volume of DDoS attacks. The authors' objectives were to overcome the limitations of reactive security systems based on intrusion detection.

They use a honeynet that performs network flow measurement, recording relevant characteristics. In this way, the authors were able to estimate the number of infected devices (bots) in the network. Based on network traffic behaviour, the number of legitimate devices and bots was estimated using regression and correlation analysis [23].

In [24] the authors presented a system that applies data mining to predict and prevent DDoS attacks on the network application layer. The aim of the work is to give priority to legitimate requests, rather than attack traffic, through a priority mechanism. This priority is given on the basis of a request classification that takes as input the history of resource use, such as CPU time, memory and disk space.

The study in [18] showed three data-driven models of the temporal, spatial and spatiotemporal behaviour of DDoS attacks, characterized by their dynamics and behaviour. These statistical models focused on predicting the occurrence of DDoS attacks, as well as botnet activities. The authors used DDoS attack traces to calculate correlations of attack characteristics (e.g. number of bots and attack duration). These characteristics are obtained by reverse engineering.

In [20] the authors explore a set of leading indicators for predicting DDoS attacks. However, their proposal presents only preliminary results. As an extension of this study, this work presents STARK, a system for predicting DDoS attacks. STARK predicts a DDoS attack before it overloads a victim (server or link), helping to prevent the network from serious consequences. Unlike other works, STARK predicts online DDoS attacks before the victim is overloaded [23].

In [27], Pelloso and Nogueira used leading indicators to detect the presence of volumetric DDoS bots on the network. Their work, however, did not focus on identifying the nodes that could be the origin of the attack, but only to the conclusion that leading indicators can provide early signals that a DDoS attack could occur in the near future.

In [28], the authors used decision tree, KNN (K-nearest neighbor), Naive Bayes and Deep Neural Network (DNN) machine learning techniques to detect DDoS attacks on cloud computing infrastructure, with an integrated OpenStack firewall and raw socket programming to monitor network traffic [19][20].

Finally, in [22], Sharyar Wani & al. use Blockchains for DDoS attack mitigation.

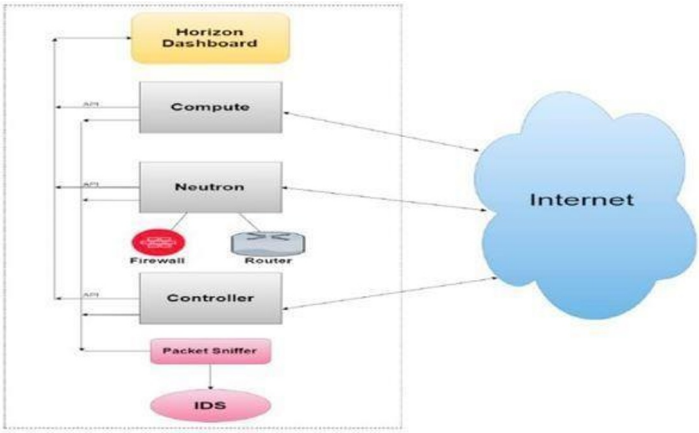

Fig. 3. OpenStack system model

4.2 Defence against malware

Malware is increasingly used in attacks against critical infrastructures; detecting it in time can help protect against such attacks.

The latest research on malware detection uses machine learning and deep learning methods. For example, the authors of [23] have implemented an automatic detection engine based on a deep neural network to detect malware. They have extracted the complete static characteristics of applications and use them to train detection models, enabling malware families to be detected.

Kan & al. in [24] have devised an approach to malware detection based on deep learning. To achieve effective malware detection on, the authors performed instruction analysis on decompiled code in order to classify the assembled instructions into different groups.

The authors of [20] introduced a malware detection method using the malware image and deep learning. First, they generated images of benign files and malware. Then, to detect malware, the authors used a deep learning method based on convolutional neurons, as this model learns the characteristics of the images.

Vinayakumar & al. in [25] have designed a malware analysis system called ScaleMalNet to detect, and accurately classify malware into its corresponding software family. ScaleMalNet is a highly scalable framework that incorporates self-learning techniques to analyse malware. It uses both static and dynamic analysis in the first stage. Malware detected in the first stage passes into the second stage to classify it into the corresponding malware family.

In [22], the authors proposed Deep Flow, a new approach based on deep learning to identify malware directly from data streams in the Android application. This approach has been tested on thousands of benign and malicious software. Experimental results have shown that this approach outperforms traditional machine learning-based approaches [26].

For Ransomware malware, recent work has been carried out for the detection of such software. Thus, in [25] the authors have proposed several preventive procedures aimed at reducing ransomware infection. These include constraining and monitoring "access to cryptographic tools". These preventive methods were not suitable for advanced ransomware [15].
The latest countermeasures consisted in applying a new strategy - the use of the NIZK proof, involving "the coexistence of private and public keys" before the encryption stage begins [27]. Another approach has been proposed by Luo & al [28]] and [29]. They propose a proactive framework consisting of policies and procedures, control and management, exposure analysis and reporting, awareness and education. They set out a generic prevention method that can be applied to any sector. This method aims to mitigate the effect of the attack by restoring the extorted files from a backup. To overcome the attack, the victim must revert to the previous (or older) version of the files [12]. Although this type of attack can save data, if the intended victim is naïve and unsophisticated, it cannot be saved.

5 Conclusion

The current world is increasingly connected to the Internet. Today, with the digital revolution, businesses, corporations, governments as well as infrastructures are all interconnected through the Internet network.
As a result, our critical infrastructures are vulnerable to attacks, some of them on a massive scale.
It is essential to secure the gateways to the Internet for these infrastructure management networks, and to set up regional or national bodies responsible for protecting critical infrastructures.
Today, many countries are taking initiatives to counter cyber-attacks, even if certain attacks such as DDoS are difficult to thwart for the time being.

References

1. Piotr Lis and Jacob Mendel. *Cyber security of critical infrastructure: an economic perspective*. Economics and Business Review, Volume 5 (19), Number 2, 2019.
2. John Moteff, Claudia Copeland, and John Fischer "Critical Infrastructures: What Makes an Infrastructure Critical?
3. Zhang, Chi & Ramirez-Marquez, José Emmanuel & Wang, Jianhui, 2015. "Critical infrastructure protection using secrecy – A discrete simultaneous game," European Journal of Operational Research, Elsevier, vol. 242(1), pages 212-221
4. Politique régionale de protection des infrastructures critiques de la CEDEAO
5. Directive 2008/114/CE du Conseil, du 8 décembre 2008, concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.
6. Thiaca THIAW, La Protection des Infrastructures, Ressources et Activités d'Importance Vitale : Législation et Pratiques au Sénégal

7. Conseil des Technologies de et des Communications (CTIC). *Infrastructures critiques dans une économie hyperconnectée.* Aout 2016.
8. Jean-Franc¸ois PILLOU et Jean-Philippe BAY. *Tout sur la sécurité informatique*. Livre, DUNOD, 4eme ` edition, Février 2016.
9. https://www.bloomberg.com/news/features/2019-12-20/spidermanhacker-daniel-kaye-took-down-liberia-s-internet
10. Michael Holloway. *Stuxnet Worm Attack on Iranian Nuclear Facilities*. Stanford University, July 2015.
11. W. Broad, J. Markoff, and D. Sanger," Israeli Test on Worm Called Crucial in Iran Nuclear Delay," New York Times, 15 Jan 11.
12. B. Kesler," The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights 10, 15 (2011).
13. L. Constantin," S. Korean manufacturing industry targeted with new backdoor program," Computer World, 2015.
14. Trend Micro," Kansas Hospital Hit by Ransomware, Extorted Twice, "Security News, 2016.
15. W. J. W. Cox," "MedStar Health turns away patients after likely ransomware cyberattack," Washington Post, 25 May 2016
16. R. Winton,""Hollywood Hospital pays 17,000 dollars in bitcoin to hackers; FBI investigating," L.A Times, 2016.
17. https://siecledigital.fr/2019/07/26/lafrique-du-sud-a-ete-visee-parunegigantesque-cyberattaque/
18. A. Wang, A. Mohaisen, and S. Chen, "An adversary-centric behavior modeling of DDoS attacks," in ICDCS. IEEE, 2017,
19. M. Nogueira, A. A. Santos, and J. M. F. Moura, "Early signals from volumetric DDoS attacks: An empirical study," arXiv, vol. 2, 2017.
20. B. M. Rahal, A. Santos and M. Nogueira," A Distributed Architecture for DDoS Prediction and Bot Detection," in IEEE Access, vol. 8, pp. 159756-159772, 2020, doi: 10.1109/ACCESS.2020.3020507.
21. K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil and D. G. Narayan," Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud", Procedia Comput. Sci., vol. 167, pp. 2297-2307, Jan. 2020.
22. Sharyar Wani, Mohammed Imthiyas, Hamad Almohamedh, Khalid M Alhamed, Sultan Almotairi," Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight", Symmetry 2021, 13, 227. https://doi.org/10.3390/sym13020227. and Yonis Gulzar
23. D. Li, Z. Wang and Y. Xue," Fine-grained Android Malware Detection based on Deep Learning," 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, 2018, pp. 1-2.
24. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran and S. Venkatraman," Robust Intelligent Malware Detection Using Deep Learning," in IEEE Access, vol. 7, pp. 46717-46738, 2019.
25. Dali Zhu, Hao Jin, Ying Yang, D. Wu and Weiyi Chen," DeepFlow: Deep learning-based malware detection by mining Android application for abnormal usage of sensitive data," 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, 2017, pp. 438-443.
26. Hackers Enigma," McAfee Labs Threats Report – June 2018," McAfee Labs, 2018.
27. S. G. Raj Samani," McAfee Labs Threats Report," McAfee Report, p.27, June 2018.
28. Q. L. X. Luo," Awareness Education as the key to ransomware prevention,"

Information security, vol. 4, no. 16, pp. 195-202, 2008

29. Q. L. X. Luo," Ransomware: a new cyber hijacking threat to enterprises," Handbook research on information security and assurance, vol. 1, no. 1, pp. 1-6, 2008