Scholar J Computational Science

Research Article

Cybersecurity Strategy to Curb Data Insecurity and DDoS Attacks on e-government for National Development

Agozie Eneh[1], Deborah Uzoamaka Ebem[2]and Uriah Auzhioluka Nwocha[3]

[1,2,3]Department of Computer Science, University of Nigeria, Nsukka, Nigeria.

[3]Department of Computer Science, Federal University of Education, Kontagora, Nigeria.

Received 1 August 2024; Acceptance 9 September 2024; Published 11 September 2024.

Abstract

As sensitive data is increasingly being shared within government agencies, organizations and across organizational boundaries, it requires persistent protection from interception and viewing by unauthorized persons. Undoubtedly, the growth and rapid adoption of the Internet has greatly changed how all organizations deal with their respective stakeholders. As the move from administrative operations to service operations accelerates, e- government Network Platform has become a solution to transform the way they do business and render services. This paper x-trays data insecurity and Distributed Denial of Service (DDoS) attacks on e-government. The paper discussed DDoS attack types on data and Information and Communication Technology infrastructure such as networks, server, computer, network devices and so on. The paper also highlighted security threat, risks, and vulnerability in e-government; economic cost of security breaches, cybersecurity concerns and mitigation of data insecurity and DDoS attacks. Recommendations made include encryption when possible, cautious biometric utilization and revisit on the national cybersecurity strategy. In addition, organizations must ensure that their document management systems and practices can safeguard personal information contained in documents throughout their life cycle.

***Keywords**:* Data Security, DDoS Attack, cybersecurity and e-government

Introduction

Security of data especially in this information age where basically humans, organizations and nations rely on the Internet is highly threatened on daily basis. From identity theft, malicious acts by hackers and crackers, to Distributed Denial of Service attacks; countries are plaque. A hacker **uses computer, networking or other skills to overcome a technical problem or to gain unauthorized access to**

Correspondence to: Uriah Auzhioluka Nwocha, e-mail: nwochaau@yahoo.com

How to Cite: Eneh et al. (2024). Cyber Security Strategy to Curb Data Insecurity and DDoS Attacks on e-government for National Development. *Scholar J Computational Science,* **1(9)**. DOI: 10.5281/zenodo.13748290

systems or networks. Hackers can have different motives, such as installing malware, stealing or destroying data, disrupting service, finding software vulnerabilities, or exploring or testing methods for breaching defenses and exploiting weaknesses [1]. On the other hand, a cracker is a person who enjoys trying to gain unauthorized access to computer systems. That means they are a kind of low-tier hacker, not out to do damage or steal information, but merely to prove their own skills. They often leave a sort of calling card to prove their success either to themselves or within their community. While many crackers are not out to harm the sites they crack, some definitely are, and they pose a security risk for their targets. Whether crackers are necessarily malicious or not, their security breaches are illegal, and even ones that only want to test their skill negatively affect the sites they hit [2]. Obviously, any sort of hacking can compromise websites and the data on them. The author in [3], asserted that government agencies are a prime target for cybercrime. Agencies hold so much diverse data about citizens — from passport information to social care data. In addition, many of them rely on the data security built for their outdated computer systems. So, cyber criminals often view government agencies as an easy mark. More concerning, public-sector groups appear to have a tough time knowing when they've been attacked. Reports shows that the United States and some countries in Europe, Asia, Middle East and even in Africa are taking proactive steps at checkmating threats to their national security by latching onto revolutions in ICT [4]. Nigerians watched in amazement how America deployed its security system to track down the April 13, 2013 Boston Marathon bombers. Similarly, in less than five minutes the images of the two men who hacked down a brave soldier on London Street on May 22, 2013, appeared on television screen around the world. There were no guess works in those scenarios, which make many Nigerians get disturbed by the many cases of unresolved high-profile crimes in the country. Riding on the skills acquired through practicing as a cracker or hacker, a serious security threat that will form the kernel of our discussion is Distributed Denial of Service (DDoS) attacks. It's a serious threat to data in the cloud and a thorn in the cyberspace. It has disrupted Quality of Service (QoS) delivery through e-governance.

Clarification of Conceptual Terms

As used in this paper, the clarification of conceptual terms is handled in this section.

National Security

National Security refers to the protection of a nation and its people from all forms of existential threats, such as economic, political, social, ecological, military, technological, or psychological [5]. According to [6], National Security is "the aggregate of security interests of all individuals, political entities, human associations, and ethnic groups which make up the nation". Also, [7] opined that National security has to do with the safety of a nation against threats such as terrorism, war, or espionage. It deals with safeguarding the sovereign, independence, and territorial integrity of the state and its citizens. National security suggest security from threats or attacks from people, organizations or countries that impact the well being of a nation and its citizen as a whole rather than of any specific individuals or within the nation. Such threats and attacks are usually directed at harming the lives of people and property [8].

Measures taken to ensure national security include using diplomacy to rally allies, using economic power to facilitate cooperation, maintaining effective armed forces, and using intelligence and counterintelligence services to detect and defeat internal and external threats. National security is the assurance of the basic conditions that guarantee the state and human security of a country **[9]**.

Data/Information Security

By *data* we mean unprocessed or raw facts such as score, time, amount, age height and so on. On the other hand, information is the product of processed data. However, what serves as information at one point can serve as information at the next level, necessarily. In twenty-first Century, the ICT has quickly spread throughout into each field of human community. Shape the Large national or international fields to the small families or people, increasingly individuals‟ utilization of information innovation to offer advantageous, quick and effective work and business. Gradually we have entered into another world, the information age. In any case, the data framework advancement is a "twofold edged sword". It made tremendous advantages for the humanity; in the meantime, the issue of data security was to bring an extraordinary misfortune and burden.

E-government Concept

E-government is the use of ICT tools and applications, whether it is Internet-based or non-Internet based to make better interaction through different delivery models and activities between government and citizens (G2C), government and business/commerce (G2B), between government agencies (G2G), or government and households (G2H) but it may face a number of limitations that affect the mode of interaction [10]**.** E-Governance is the outgrowth of the efforts made by the governments to improve relations with their citizens. If certain conditions are fulfilled, the legal value of electronic transactions shall be equivalent to that of other forms of communication, such as the written form. To protect E-Governance projects there is need for information security best practices. Security polices, practices and procedures must be in place as well as utilization of security technology, which help to protect e-Government systems against attack, detect abnormal activities services and to have a proven contingency plan in place [11-12].

Cybersecurity

Computer security, cybersecurity (cyber security), or information technology security (IT **security**) is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide [13-14]. The field has become of significance due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi and due to the growth of smart devices, including smart phones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance [15].

Distributed Denial of Service (DDoS) Attack

A DDoS attack is a coordinated **cyber attack on a server, service, website, or network that floods it with Internet traffic.** It is a large scale coordinated attack on the availability of services of a victim system or network resources launched indirectly through many compromised computers on the Internet called Zombies. It is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. More sophisticated strategies are required to mitigate this type of attack, as simply attempting to block a single source is insufficient because there are multiple sources.

Historical Background of DDoS attacks

Network in the world of computers is said to be a collection of interdependent hosts, via some shared media which can be wired or wireless. The global interconnection of these computers is referred to as the Internet. This interconnection among computers facilitates information sharing among them [16]. According to [17], the first-ever Denial of Service (DoS) attack occurred in 1974 courtesy of David Dennis, a 13-year-old student at University High School, University of Illinois. Since the first DoS attack was launched in

1974, DDoS attacks and other DoS attacks have remained among the most persistent and damaging cyber-attacks.

One of the first large-scale DDoS attacks occurred in August 1999, when a hacker used a tool called "Trinoo" to disable the University of Minnesota's computer network for more than two days. Trinoo consisted of a network of compromised machines called "Masters" and "Daemons," allowing an attacker to send a DoS instruction to a few Masters, which then forwarded instructions to the hundreds of Daemons to commence a UDP flood against the target IP address. The author [18], averred that the biggest DDoS attack to date took place in September of 2017. The attack targeted Google services and reached a size of 2.54 Tbps. Google Cloud disclosed the attack in October 2020. Also, in the year 2000, a 15-year-old hacker known as 'Mafiaboy' took down several major websites including CNN, Dell, E-Trade, eBay, and Yahoo!, the last of which at the time was the most popular search engine in the world. This attack had devastating consequences, including creating chaos in the stock market.

One of the solutions to have a successful attack is to distribute the attack among a group of computers around the network. Moreover, tracing an attack originated from multiple sources is a daunting task.

Principles and Components of DDoS Attack

A DDoS attack consists of four (4) main components usually deployed in launching attacks. They are:

- The master or main attacker;
- the handler;
- slave computers or zombies; and
- the victim computer.

The main attacker initiates the attack from the master computer and tries to find some slave computers maliciously empowered by the handler to be involved in the attack.

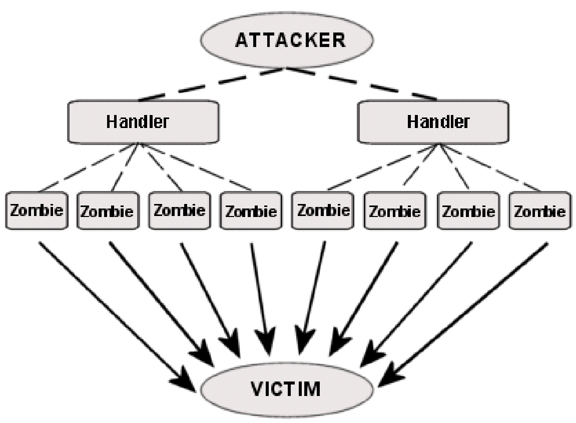

Figure 1. Architecture of a Distributed Denial of Service Attack

A small piece of software is installed on the slave computers through the handler to run the attacker commands. The attack scenario continued through a command issued from the attacker resides on the master computer toward the slave computers to run their pieces of software. The mission of the piece of software is to send dummy traffic destinated toward the victim. Therefore, the victim will not be able to do anything to prevent this attack. To reduce the network traffic, the victim should detect the attack just in time to be able to block some IP addresses. Detection of an attack on time has an important role in preventing the progress of the attack. As DDoS attack generation tools and methods try to increase traffic toward the victim computer using generating normal packets, signature based intrusion detection systems are unable to detect such attack [19].

A DoS was made from a system or network while a DDoS attack is organized to happen simultaneously from a large number of systems or networks. The denial of service attack, generated by utilizing the vulnerabilities in the network protocol affects the performance of the victim as well as the other hosts sharing the network.

DDoS Attack Types on Data and ICT Infrastructure

Distributed Denial of Service (DDoS) on data and computer infrastructure attack includes different types of attacks. Descriptions of those attacks on the Internet are presented below [20]:

Smurf attack

In this attack, the attacker sends a large number of Internet Control Message Protocol (ICMP) echo requests to the server. The victim server will be flooded with broad cast addresses since the sender IP address is the broad cast IP address. The Smurf attack is executed using the following steps:

i. An attacker sends packets to a network device that supports broadcast addressing technique e.g. Network amplifier. The return address in these packets is forged or spoofed with victim's address.
ii. ICMP_ECHO_RESPONSE packets are sent by the network amplifier to all the systems in the Broad-cast IP address range.
iii. An ICMP_ECHO_REPLY message from all the systems in the range reaches the victim.

IP Spoofing attack

Internet Protocol (IP) spoofing attack occurs when the attacker modifies the headers of source IP field either by a legitimate IP address or by an unreachable IP address. When this happens, the cloud server will be misguided to the legitimate client and in turn it affects the genuine user or the server will be unable to complete the task to the unreachable IP address which affects server resources. Preventing this type of attack is difficult due to the fake IP address of the source IP.

Teardrop Attack

In a network transmission, IP packets are broken down into smaller chunks and each fragment will have the original IP packet's header that will be useful to re assemble at the destination host. It is known that when the TCP/IP stack is overlapped with IP fragments, the re assembling will be a very difficult and sometimes it can quickly fail [20]. To avoid this attack, most of networks use firewalls which can block tear drop packets in return since this makes it disregard all broken packets. Of course, if you throw a ton of Teardrop busted packets at a system, it can still crash many other variants such as Targa, SynDrop, Boink, Nestea Bonk, TearDrop2 and NewTear are available to accomplish this kind of attack.

SYN Flood attack

The SYN Flood attack happens when the attacker machine sends a flood of TCP/SYN packets with a fake IP address. In a TCP/IP handshaking process, each of these packets is treated like connection request. So the server sends back a TCP/SYN_ACK packet and waits for a packet in response from the sender IP address. Since the sender IP is a fake, the response to the ACK packet never comes. As a result, it causes to half-open connections [3]. These half-open connections saturate the number of connections to the server so that it avoids responding to the legitimate requests.

PING of Death attack

A ping of death involves sending a malicious ping to a computer. The pin is generally of 32 bytes in size. The attacker sends a packet with a size greater than the limit of the IP protocol 65,535. Handling an oversized packet affects the victim's machine inside the cloud environment and its resources. Many operating systems had problems of what to do when they received an oversized packet, so crashed, or rebooted. Many new variants of ping of death include jolt, sPING, ICMP bug, IceNewk, Ping o' Death [21-22].

Buffer Overflow Attack

The attacker sends an executable code to the targeted system in order to create buffer overflow attack. In such way, the victim's machine will be controlled by the attacker. As a result, the attacker can use the infected machine to perform cloud based DDoS attack.

LAND Attack

It is similar to ping attack where it uses "land.c" program to send the modified TCP/SYN packets with the victim's IP address in both source and destination IP fields. As a result, the machine itself sends the requests and crashes. DDoS attacks are highly distributed, offensive assaults on services, hosts and infrastructure of the Internet.

Security Threats, Risks, and Vulnerability in e-government

In the designing of an efficient e-Government system, security becomes the main issues to be considered. E-Government system is the type of on-line system that requires an ICT based network to execute properly but e-Government system is different from other on-line system particularly with reference to security as it handles a lot of secure and legal information that must be protected [23]. A few researchers have attempted to define each of threats, risks, and vulnerability individually. In any case it is the interactive relationship of every one of the three of these parts that merge to make the fundamental assessment and suggested action plan for risk administration. The author [24], asserted that as the individual responsible for the oversight of the security of an agency, the more you excuse this procedure like an expert with high level security expertise, the better your knowledge and clarification of the after effects of their security reviews, and capability to execute their discoveries in a way most suited to one's agency or establishment.

Risk refers to the probability of being focused by a given attack, of an attack being effective and generally present to a given threat. A risk assessment is performed to decide the most important potential security breaches to address now, as opposed to later [19]. However, threat is anything being influenced or harmed by a particular thing, deliberately or by mistake, and can damage or destroy an asset. Off course asset is what we are attempting to protect. Vulnerability is weaknesses or gaps in a security program that can be used by threats (attacker) to obtain unauthorized access to an asset [25]. Figure.2 shows the need for secure relation between citizens and agencies through e-government.

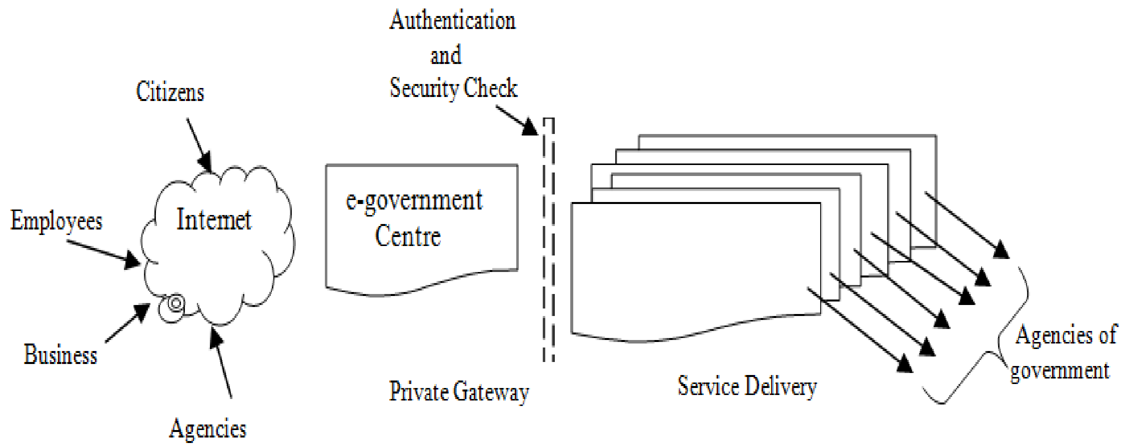

Figure 2. Securing Service Delivery

Nature and Importance of Data Security and Cybersecurity

Securing the confidentiality, integrity and availability of information assets is the crux of the matter. The terms data security and cybersecurity are often used interchangeably because both seek to protect information assets (valuable data and information) and secure technology assets (hardware, software, systems, servers, networks and other electronic containers that collect, process, transport, store and retrieve information assets). The distinction is subtle, with data security emphasizing direct protection of information assets themselves and cybersecurity emphasizing securing technology assets as a means to protecting information assets. According to [22], both data security and cybersecurity seek to maintain the confidentiality, integrity and availability of an organization's information assets. In this context, confidentiality means ensuring access to information assets is limited to authorized persons and systems; integrity means ensuring information assets remain in the condition intended by the owner; and availability means ensuring reliable access to information assets by authorized persons and systems. These three security pillars are known as the CIA triad.

A security incident is an event that compromises the integrity, confidentiality or availability of information assets, a data breach is a security incident that results in disclosure of confidential data to an unauthorized person, and a cyberattack is an unauthorized attempt by a threat actor to compromise information or technology assets. Security threats to information and technology assets today are wide-ranging and evolving [24]. The growing importance of information and technology assets Public and private enterprises are amassing massive and growing volumes of information assets as individuals are also increasingly creating, collecting, sharing and consuming data. Enterprises and individuals rely increasingly on information and technology assets to provide or procure goods, services and information. Enterprises and individuals are also entrusting their information to other enterprises or individuals at growing rates.

In both high income and developing countries, individuals are embracing digital technologies. For example, there have been multiple security incidents related to digital financial services, such as unauthorized third-party access to corporate information systems gained by luring unsuspecting employees to disclose user login information in Ghana, Kenya, Tanzania, Uganda and Zambia, an outage during a system upgrade in Zimbabwe, and a malicious denial-of service attack in Kenya [23,26].

The Economic Cost of Security Breaches

The global direct monetary losses from cybercrime in 2020 were estimated to have nearly doubled to USD 945 billion from USD 522.5 billion in 2018, while spending on cybersecurity in 2020 was expected to exceed

USD 145 billion, together comprising 1.3% of global GDP. In 2017, cybercrime cost Africa an estimated USD 3.5 billion in direct losses [27]. These estimates exclude indirect costs to victims such as opportunity cost, downtime, lost efficiency, brand disparagement, loss of trust, intellectual property infringement, and damage to employee morale. They also exclude systemic costs such as supply chain impacts on upstream suppliers and downstream customers. The full economic cost of cybercrime, including direct, indirect, and upstream systemic costs, has been estimated at three times its direct cost30 – putting 2020 total global cost near USD 4 trillion, about 4% of global GDP.

Enactment of National Cybersecurity Strategy

Facing these challenges, many governments have adopted a national cybersecurity strategy, which is an action plan to improve security and resilience of national infrastructure and services. These strategies reflect high-level, top-down approaches to cybersecurity that establish national objectives, priorities, and timelines [27]. The first national cybersecurity strategy, the US Government's National Strategy to Secure Cyberspace, was released in February 2003 after the 11 September 2001 terrorist attacks on the World Trade Center. 50 Cybersecurity plans with more limited focus were adopted in Germany and Sweden in 2005 and 2006. The world's second broad national cybersecurity strategy was published by Estonia in 2008 following a severe cyberattack in 2007. At least 114 countries have adopted or are in the process of adopting a national cybersecurity strategy, including 17 in sub-Saharan Africa, 18 in the Americas, 11 Arab states, 21 in the Asia-Pacific, 6 in the Commonwealth of Independent States, and 41 in Europe [18].

Mitigating Data Insecurity and DDoS Attacks

To foster national development, government can mitigate data insecurity and DDoS attacks as follows:

i. ***Improvement on ICT Infrastructure***

Relying solely on passwords for security has resulted in many organizations experiencing cyber attacks. Employing software that limits access to organization networks is a key step for governments to avoid such attacks. Two-factor authentication, biometrics and encryption are some of the components necessary in such solutions.

ii. ***Implementation of Adaptable Authentication Methods***

Phishing has been one of the most alarming forms of security breaches. Users are tricked into revealing important information. Governments are tackling phishing attempts with multifactor authentication. They also need to ensure that the authentication system used supports mobile interfaces and is made with mobile users in mind.

iii. ***Effective and Cautious Biometrics Utilization***

Biometrics is used for individual authorization, providing access and identifying individuals. The use of biometrics with digital devices has improved their security. For example, biometrics such as fingerprint and facial recognition helps ensure that no one except the intended user can unlock the device.

iv. ***Audit and Identify Shared Assets***

Third-party attacks happen when cybercriminals enter your system through an outside partner, making third-party authorization a risky process. Because of this, governments should perform third-party audits and implement cybersecurity solutions built to identify all third-party user activity. A shift to remote work after Covid-19 increased the number of opportunities for attackers.

v. ***Encrypt When Possible***

Encryption allows the integrity of data to be maintained by turning simple text into an encrypted code language. Encrypted data isn't understandable by humans—it can only be deciphered by computers and decryption tools.

vi. **Training and Retraining of Personnel**

Training employees on password management and how to avoid phishing emails is one part of the solution. It's important for governments to adopt a culture of cybersecurity at all levels: leadership, teams and individuals.

vii. **Periodic Revisiting of Security Policies**

There's a need to have a zero-tolerance policy toward cybercrimes. As attacks become more sophisticated, they must also put strong policies in place that enable employees to detect, respond and recover from such attacks.

Recommendations

i. Fundamental factors are to have a proper public key infrastructure providing required level of authentication and integrity.

ii. have a continuous awareness and training program to ensure people understand security threats, know how to identify potential issues and behave accordingly to maintain a secure e-Government service.

References

1. Stallman, R. (2020). "The Hacker Community and Ethics: An Interview with Richard M. Stallman". GNU Project. Available at http//:www.gnu.org/philosophy/rms-hack.html.

2. Hawthorne M. (2019). Technipages Explains Cracker. What is Cracker? definition & meaning - Technipages. Available at http//:www.technipages.com/definition/cracker/
3. Brown, J. (2021). Roundup: Government Data Security Threats in 2021. Available at http://www.securityintelligence.com/articles/government-cybersecurity-threat-roundup- 2021/
4. Thisday (12 Sept. 2013). Addressing National Security Challenges with Technology Tools. Published by: Thisday Newspaper Saturday September 12, 2013 Nigeria. Available at: http://www.thisdaylive.com/articles/addressing-national-security-challenges-with technology-tools/158831/
5. Okoli, A. C & Okpaleke, F.N. (2014). Cattle rustling and dialectics of security in northern Nigeria. *International Journal of Liberal Arts and Social Science*, 2 (3), 109-117.
6. Obasanjo, O. (2012). Constructive engagement. http://www.conference.bigdatanigeria.org/wp-content/uploads/2016/08/SOCIAL-MEDIA-AND-NATIONAL-SECURITY-IN- NIGERIA.pdf
7. Ebere, N. (2017). Social Media and National Security. Retrieved from https:/www./Social%20Media%20and%20National%20Security%20_%20Raadaa.html
8. Adams, O. K. (2016). The role of information technology in national security: "a case study of Nigeria". *Global journal of computer science and technology: information & technology,* 16(1). https://globaljournals.org/gjcst_volume16/2-the-role-of-information-technology.pdf
9. Okoli, A. I. C. & Idom, A. M. (2018). The internet and national security in Nigeria: a threat- import discourse *covenant university journal of politics & international affairs. 6(1).* http://journals.covenantuniversity.edu.ng/index.php/cujpia/article/viewfile/1246/776
10. Valentina, N. (2004) E-government for developing countries opportunities and challenges, EJISDC, 18, 1, 1-24 31)
11. Alharbi, k, (2013). E-government security modeling: Explaining main factors and analyzingexisting models, International Journal of Social, Human Science and Engineering, *(7)2,* pp*. 134-140.*
12. Al-Khouri1, I. M. (2013). Technological and Mobility Trends in E-Government, Business and Management Research Journal, BMRJ, (*2)3*, pp. 230-238.

13. Schatz, D.; Bashroush, R &Wall, J. (2017*).* "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.*
14. Stevens, T. *(11 June 2018).* "Global Cybersecurity: New Directions in Theory and Methods" (PDF). *Politics and Governance.* ***6*** *(2): 1–4 doi:10.17645/pag.v6i2.1569. Archived (PDF) from the original on 4 September 2019.*
15. Kianpour, M.; Kowalski, S.; Øverby, H. *(2021).* "Systematically Understanding Cybersecurity Economics: A Survey". Sustainability. **13** (24): 13677. doi:10.3390/su132413677. https://www.oas.org/juridico/PDFs/cyb9coecyboasDec16_v1.pdf.
16. Siddiqui, M. N., Saini, V., Ahuja, R., Wyld, D. C., Wozniak, M., Chaki, N., Meghanathan, N., & Nagamalai, D. (2011). *Advances in Network Security and Applications*. *196*(July), 649–657. https://doi.org/10.1007/978-3-642-22540-6
17. Staff, R. (2017). *DDoS Attacks History*. https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/
18. CloudFlare. (2020). *Famous DDoS attacks | Biggest DDoS attacks Cloudflare*. https://www.cloudflare.com/en-gb/learning/ddos/famous-ddos-attacks/
19. Azahari, M., Yusof, M., Hani, F., Ali, M., Darus, M. Y., & Sciences, M. (2019). Classification Algorithm Against Different Types of DDoS Attacks Using Hybrid Approach. *International Journal of Innovations in Engineering and Technology (IJIET) Http://Dx.Doi.Org/10.21172/Ijiet.143.16 Classification*, *14*(3), 137–144. https://doi.org/dx.doi.org/10.21172/ijiet.143.16 Classification
20. Glăvan, D., Răcuciu, C. & Moinescu, N. A. (2019). DDoS detection and prevention based on artificial intelligence techniques. *Scientific Bulletin of Naval Academy*, *XXII*(1), 134–143. https://doi.org/10.21279/1454-864x-19-i1-018
21. Chen, S., Tang, Y., & Du, W. (2007). Stateful DDoS attacks and targeted filtering. *Journal of Network and Computer Applications*, *30*(3), 823–840. https://doi.org/10.1016/j.jnca.2005.07.007
22. Harshita, K. & Nayyar, R. (2017). Detection of ICMP Flood DDoS Attack. *International Journal of New Technology and Research (IJNTR)*, *5*(2), 199–205. www.ijcstjournal.org/volume-5/issue-2/IJCST-V5I2P39.pdf
23. United Nations, (2012). E-government survey 2012, E-government for the people, economic and social affairs department , ST/ESA/PAS/SER.E/150 30)
24. Lampri, M. (2012). E-Government and Data Protection in the Public Sector. In: Lazakidou, A. (eds) Virtual Communities, Social Networks and Collaboration. Annals of Information Systems, vol 15. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-3634-8_7
25. Mohan, S. (2023). Data Security for Governments: Current Challenges And The Way Forward. Forbes Technology Council; Available: http://www.forbes.com/sites/forbestechcouncil/2023/02/22/data-security-for- governments-current-challenges-and-the-way-forward/?sh=a56e1c36fef1
26. African Union (2020). African Union, List of countries which have signed, ratified or acceded to the African Union Convention on Cyber Security and Personal Data Protection (status at 18 Jun 2020).Available:https://www.au.int/sites/default/files/treaties/29560-sl-african%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf .
27. Seger, A. (2021). Council of Europe, “Implementation of the Budapest Convention on Cybercrime” at slide 3 (Meeting of the Working Group on Cybercrime, OAS Meetings of the Ministers of Justice or Attorneys General of the Americas, Washington, DC, 12-13 Dec 2016). Available: https://www.oas.org/juridico/PDFs/cyb9coecyboasDec16_v1.pdf.