ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

# Cyber Attacks and its Mitigation: A Review of Cyber Attacks on INEC IREV in the last 2023 Presidential Elections

**Oladimeji S.A., Madu F.U., Obioha I., Emeagi O.I. , Okpara E.I.**

Department of Computer Science, Federal Polytechnic Nekede, Owerri.
Department of Computer Science, Federal Polytechnic Nekede, Owerri.
Department of Computer Science, Federal Polytechnic Nekede, Owerri.
Department of Computer Science, Federal Polytechnic Nekede, Owerri.
MIS Unit, Federal Polytechnic Nekede, Owerri.

**ABSTRACT:** Nigerians have been craving more transparent, free, fair, and credible elections since the return of democracy in 1999. From the era of manual processes, the Independent National Electoral Commission (INEC) has continued to introduce technological innovations to make elections better. These innovations have not been without challenges and time has in turn brought about more advanced solutions. Shortly before the 2023 general elections, more advanced technological intervention called the Bimodal Voter Accreditation System (BVAS) and INEC Results Viewing (IREV) portal were introduced and tested. People actually believed the reliability of these technologies having been deployed and used in some elections before the general elections. As there is no technology without its vulnerabilities and flaws, political stakeholders through their sponsored attackers took advantage of the new technology and launched attacks on INEC system for the purpose of tampering with the results being uploaded onto the server. However, INEC was unable to transmit polling results to their server in real-time for public viewing. This made the opposition parties rejected the outcome of the presidential election. Although, INEC claims it could not upload to results to IREV due to huge cyber-attacks launched on INEC servers. This reason by INEC is still not clear to some citizens as very few understand how the system works. This paper clarifies and identifies some of the vulnerabilities associated with servers and also throws more light on server technology, how it works, and the need to have reliable database and network security in Nigeria.

**KEYWORDS:** INEC, BVAS, IREV, SERVER etc.

## I. INTRODUCTION

The driving force behind cyber-security is the threat of cyber-attacks. Each level of a cyber-physical infrastructure which consists of operational software, information, and people is susceptible to security breakdown, whether through attack, data breach, infiltration, or accident. Cyber threats are asymmetric because they allow few individuals to perpetrate attacks upon organizations and the masses. Through Inter-connected computer, an aggressive cyber actor may conduct a cyber-attack with minimal technical and operational resources. With a minimal chance of failure, cyber-attacks offer a high return for a low financial investment. Because of the permeable nature of sophisticated networks, a cyber-actor may infiltrate an adversary's network with minimal risk of discovery [1]. The increasing trend of ubiquitous computing with cyber threats is characterized by an attacker, a target system, a set of actions against the target, and the consequences resulting from the attacks. Consequences may include damages to the target systems and servers, direct and indirect losses to victims, and variable impact on third parties. As cyberspace becomes increasingly pervasive and entrenched in society, it spawns the availability of more targets to attack, and an increase in the population of skilled attackers [1] Defenders must familiarize themselves with the environment by understanding not only the cyber domain but also the human element, the attacker, their motives and goals. Consideration of the identified key components will provide greater fidelity to the orientation phase of the decision-making process.

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunication networks, computer systems, and

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

embedded processors and controllers. As societal dependency on information technology grows, so do cyber threats. A diverse group of Nation-states, non-state actors, state-sponsored groups, and individuals may wage malicious cyber-attacks on a target server [2] Cyber and sabotage attacks on critical INEC information technology infrastructures may be viewed by invested adversaries as a way to circumvent Nigeria strengths on the battlefield and attack states' interests directly. In support of the national security strategy, the nation must institute a multilateral strategic framework that focuses on the dynamic challenges of cyber in this information age [2]. As the technologies are new and strange to some Nigerians and INEC has continued to invest heavily on IT facilities for the betterment of our electoral system, proper and adequate awareness, through voter education programme should be given to the masses in order to be aware of how new technologies work.

## II. OVERVIEW OF CYBER ATTACKS

Cyber security is a rapidly growing field that needs a lot of attention due to remarkable developments in IoT networks, cloud and web technology, mobile world, online banking, smart grid, etc. Cloud is becoming more appealing to hackers due to its open nature and the quantity of traffic created by the cloud [3]. For example, the most prevalent cybercrime attacks after data theft are distributed denial of service (DDoS) attacks. TCP and/or UDP flood attacks can drain cloud resources, absorb much of their bandwidth, and damage a complete cloud project in a short time. These security threats include the creation and deployment of an efficient intrusion program that will protect the cloud from zero-day attacks that have just arisen. The most common challenges traditional methods face is that IDS generates false alarms and does not use appropriate standards or parameters to assess threats. [3]. This may contribute to the problem of misuse. Faster transition of data made the network an Interesting and allow access goal for attackers to hack and play with different kinds of attacks. Consequently, many intrusion detection strategies have developed to secure distributed services in the cloud by detecting the various forms of attack on the network [4]. The big benefit for the population of attackers today is the availability of open access to infrastructure and broad file and knowledge sharing networks. And so, each other day they prepare more and more new kinds of attacks. Software manufacturers who don't pay enough attention to their security modules create vulnerabilities not just to their device but also to the overall system and often become vulnerable to one malicious application for the entire network [5]. Cyber Security ensures the confidentiality of computer-connected systems, software, hardware and information from cyber-attacks. Without a protection policy in line, attacker can easily access your system and misuse your private information, customer data, business intelligence and much more. This analysis is being carried out with the aim of properly understanding the definition of cybercrime and cyber protection and of providing effective and appropriate remedies to address these concerns in today's Internet world. In addition to this, the purpose of the study is to provide a framework for new opportunities for analysis

## III. SERVER TECHNOLOGY

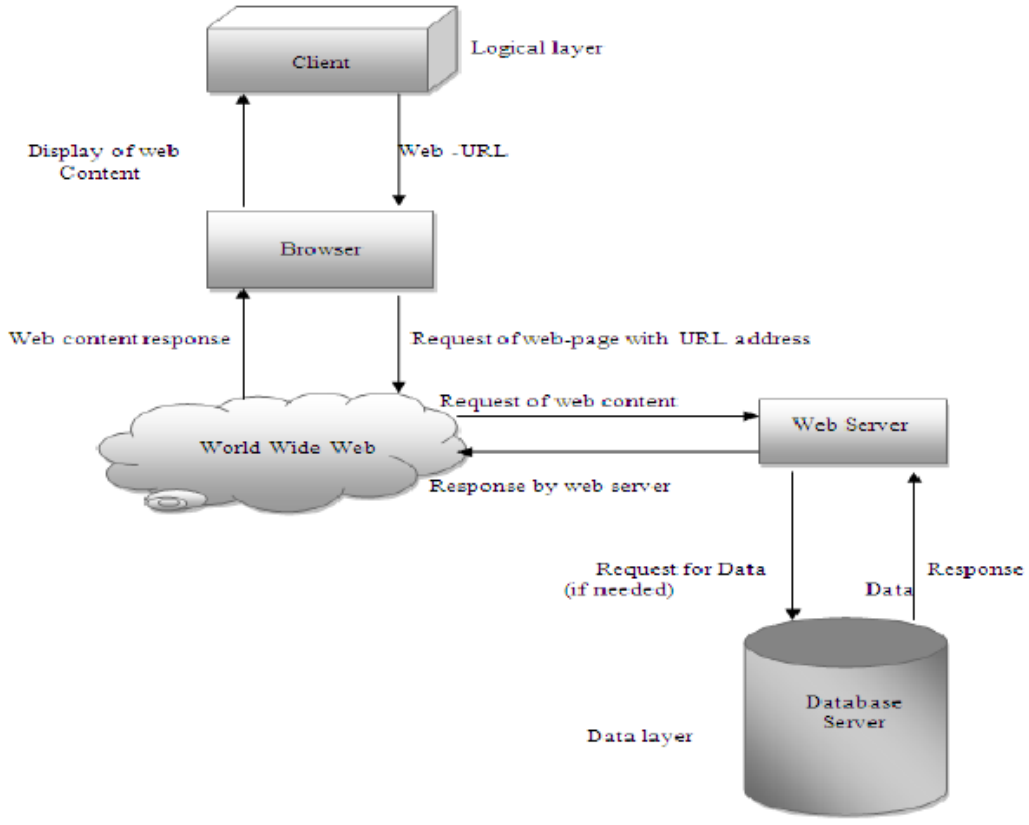
A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing and delivering webpages to users. Besides HTTP, web servers also support SMTP (Simple Mail Transfer Protocol) and FTP (File Transfer Protocol), used for email, file transfer and storage. Web server hardware is connected to the internet and allows data to be exchanged with other connected devices, while web server software controls how a user accesses hosted files. The web server process is an example of the client/server model [27]. All computers that host websites must have web server software. Web servers are used in web hosting, or the hosting of data for websites and web-based applications -- or web applications.

### Web Server Technology

Web server software is accessed through the domain names of websites and ensures the delivery of the site's content to the requesting user. The software side is also consist of several components, with at least an HTTP server. The HTTP server is able to understand HTTP and URLs [27]. As hardware, a web server is a computer that stores web server software and other files related to a website, such as HTML documents, images and JavaScript files. When a web browser, like Google Chrome or Firefox, needs a file that is hosted on a web server, the browser will request the file by HTTP. When the request is received by the web server, the HTTP server will accept the request, find the content and send it back to the browser through HTTP [26].

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

More specifically, when a browser requests a page from a web server, the process will follow a series of steps. First, a person will specify a URL in a web browser's address bar. The web browser will then obtain the IP address of the domain name -- either translating the URL through DNS (Domain Name System) or by searching in its cache. This will bring the browser to a web server. The browser will then request the specific file from the web server by an HTTP request. The web server will respond, sending the browser the requested page, again, through HTTP. If the requested page does not exist or if something goes wrong, the web server will respond with an error message. The browser will then be able to display the webpage. Multiple domains also can be hosted on one web server [27]. Web servers often come as parts of a larger package of internet and intranet related programs that are used for sending and receiving emails, downloading requests for File Transfer Protocol (FTP) files, and building and publishing webpages. Many basic web servers will also support server-side scripting, which is used to employ scripts on a web server that can customize the response to the client. Server-side scripting program runs on the server machine and typically has a broad feature set, which includes database access. The server-side scripting process will also use Active Server Pages (ASP), Hypertext Preprocessor (PHP) and other scripting languages. This process also allows HTML documents to be created dynamically [26].




**Typical diagram of web server technology (25)**

**Dynamic vs. static web servers**

A web server can be used to serve either static or dynamic content. Static refers to the content being shown as it is, while dynamic content can be updated and changed. A static web server will consist of a computer and HTTP software [25]. It is considered static because sever will send hosted files exactly the way it is, to a browser. Dynamic web browsers will consist of a web server and other software such as an application server and database. It is considered dynamic because the application server can be used to update any hosted files before they are sent to a browser. The web server can generate content when it is requested from the database. Common web servers available are:

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

I. Apache HTTP Server. Developed by Apache Software Foundation, it is a free and open source web server for Windows, Mac OS X, Unix, Linux, Solaris and other operating systems.
II. Microsoft Internet Information Services (IIS). It is not open sourced, but widely used.
III. Nginx. A popular open source web server for administrators because of its light resource utilization and scalability. It can handle many concurrent sessions due to its event-driven architecture. Nginx also can be used as a proxy server and load balancer.
IV. Lighttpd. A free web server that comes with the FreeBSD operating system. It is seen as fast and secure, while consuming less CPU power [26].
V. Sun Java System Web Server. A free web server from Sun Microsystems that can run on Windows, Linux and UNIX. It is well-equipped to handle medium to large websites.

## IV. THE INEC BVAS & IREV

The Bimodal Voter Accreditation System is an electronic device developed to read Permanent Voter Cards (PVCs) and verify the voter holding the card by using his/her fingerprints and facial recognition. The hardware components of the BVAS are shown in the image below [17].

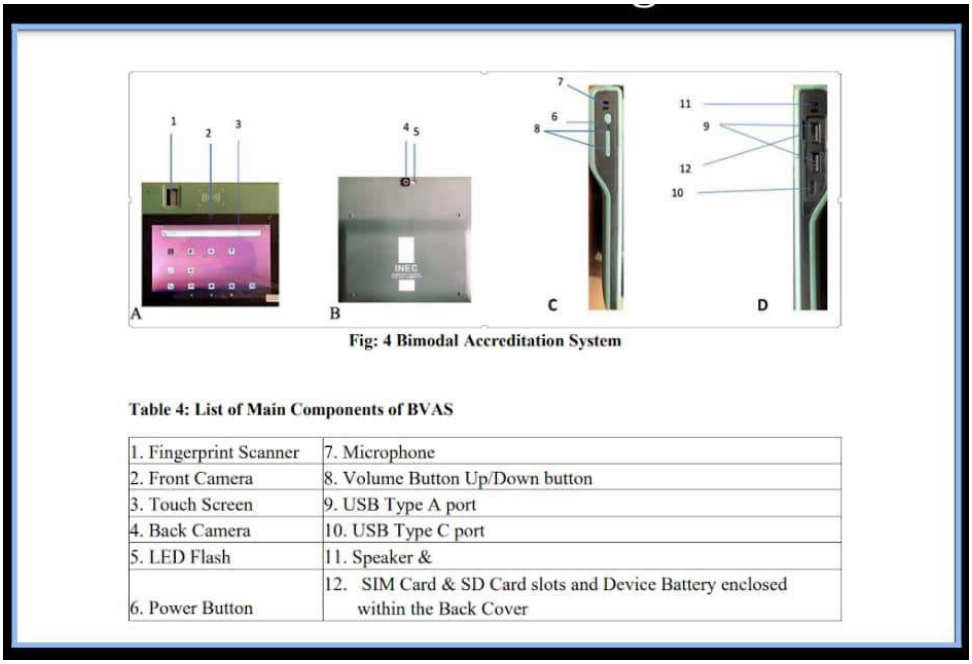



Fig: 4 Bimodal Accreditation System

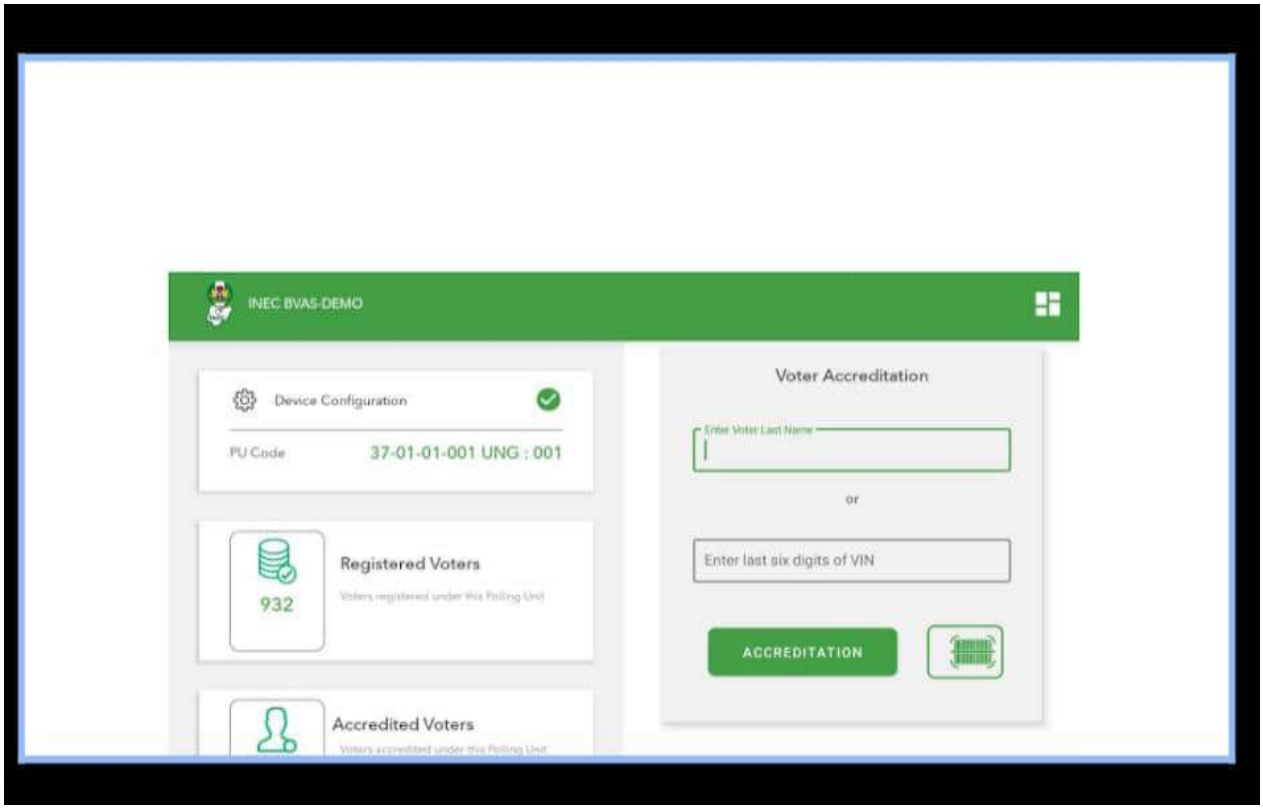
Table 4: List of Main Components of BVAS

| | |
|---|---|
| 1. Fingerprint Scanner | 7. Microphone |
| 2. Front Camera | 8. Volume Button Up/Down button |
| 3. Touch Screen | 9. USB Type A port |
| 4. Back Camera | 10. USB Type C port |
| 5. LED Flash | 11. Speaker & |
| 6. Power Button | 12. SIM Card & SD Card slots and Device Battery enclosed within the Back Cover |

Components of BVAS (source: INEC election manual)

The image below shows the BVAS election dashboard with all the key options to begin voter accreditation. It shows Polling Unit information, the total number of registered voters, and the total number of accredited voters [17].

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023



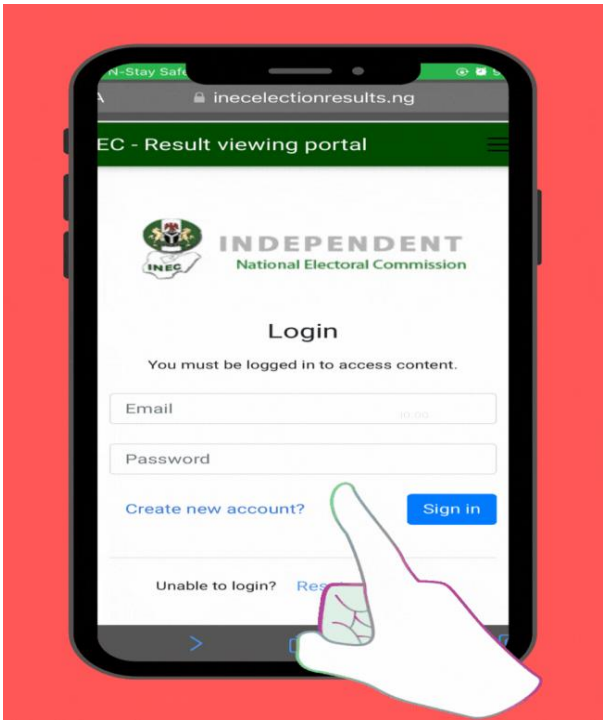

BVAS election dashboard (Source: INEC election manual)

Apart from the above function, the BVAS will also be used to transmit a snapshot of the result sheet at polling units to the INEC portal in real time for the public to see, as long as they are logged in to the portal. One of the challenges faced in the electoral process is the irregularities that take place between the Polling Units (PUs) and the result collation centers. Results are, sometimes, hijacked, changed, or even destroyed [18]. This led INEC to considering using the BVAS technology in transmitting the results directly from the PUs. This system minimizes human error and delays in results collation. It also improves the accuracy, transparency, and credibility of the result-collation process. This, therefore, implies that the BVAS must first read a voter's PVC and authenticate him/her as the rightful holder of the card before the person would be able to vote on election day. Voting will be impossible without the two-step verification [19]. The BVAS machine works offline and does not rely on the internet to accredit voters on election day but it will require a network connection for the transmission of results to INEC IREV.

**The INEC IREV**

Nigeria's 2023 elections are experiencing record-breaking voter participation and high voter confidence. One of the few reasons may include the implementation of technology in the electoral process, such as the INEC Election Result Viewer [20]. The INEC Result Viewing Portal (IReV) is a platform created by the Independent National Electoral Commission (INEC) in Nigeria to provide real-time transmission of election results from polling units to the central collation centre. It was designed to enhance the transparency of the electoral process and reduce the incidence of vote rigging and election manipulation. The IReV platform allows voters and other interested parties to monitor the electoral process and view the results of ongoing elections in real-time [17]. The portal provides pictures of the election results from each polling unit, including the number of votes cast for each candidate and the percentage of total votes cast. Here is how you can access the result viewing portal:

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

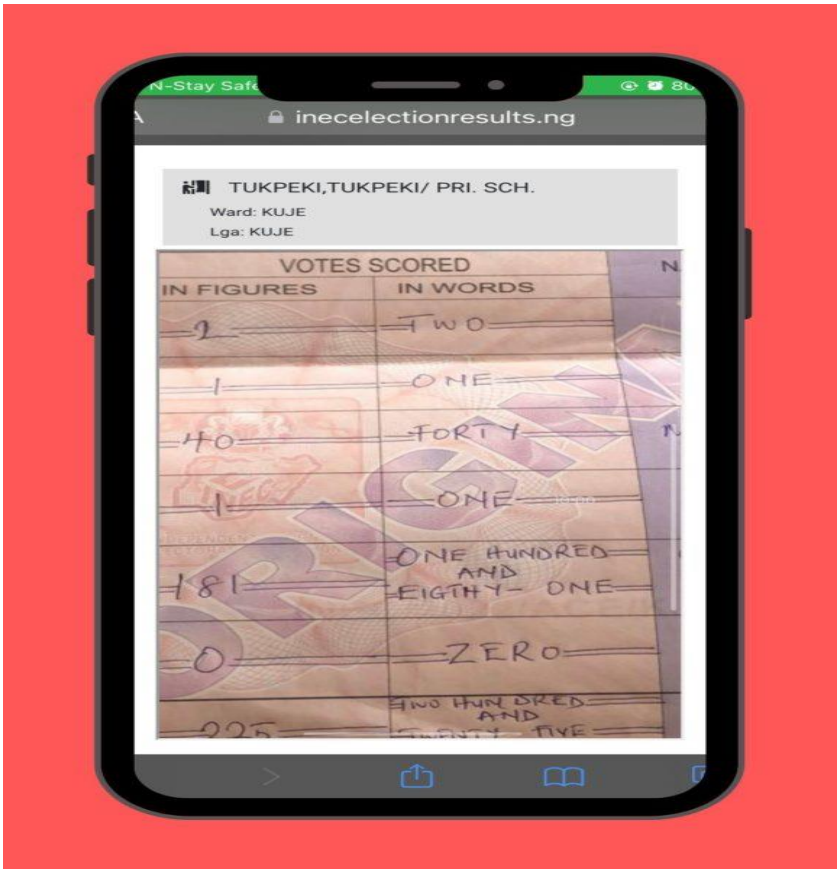



How to register to use the INEC result portal. (Image source: TechCabal) [17]

I. Visit the website of the INEC Result portal; http://inecelectionresults.ng
II. Log in if you have used it in past elections. If it is your first time using the result portal you need to create an account. Click "Create new account."
III. Enter all the required fields and sign in.
IV. A six-character activation code will be sent to your email address. Go to your email, copy it and paste it into the field that requires it. Then click activate.
V. You will be immediately logged in and led to the Result Console. There you will see tabs labelled presidential election, governorship election, senatorial election, House of Representatives election, state House of Assembly election, Chairmanship election and Councilors.
VI. Click on the election of your interest and you select the state, the LGA, the ward, and the polling unit. It is the polling unit results that are uploaded and they are uploaded as images pictures of the ECr8 Form where presiding officers write the ballot vote counts.
VII. You can also have access to results from previous elections like the Ekiti, Osun, and the FCT Area council election [16][17]

The results you see on the web-based IReV were transmitted from the Bimodal Voters Accreditation System (BVAS). Both technologies were introduced in 2021 [17]. The BVAS doubles as an accreditation device to verify that the PVC of a present voter is valid and to certify that the results of the election are valid and there are no occurrences of over-voting. It is also a photography device to capture pictures of results and upload them to the IReV.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023




A result on the IReV (Image source: TechCabal)

The results of voting in each polling center are handwritten on a form, and the BVAS takes a picture of the form, which is filled out and signed by the presiding officer at that polling unit. The picture is uploaded to the IReV and saved as a viewable PDF file, and it is accessible via the internet from anywhere in the world[17][18]. However, the effectiveness of the IReV platform is dependent on the availability and reliability of the internet network in Nigeria.

## V. ATTACKS ON INEC SERVER BEFORE AND DURING THE 2023 GENERAL ELECTIONS

Ministry of Communications and Digital Economy has said while monitoring the cyberspace, about 12.9 million attacks were launched against servers of the Independent National Electoral Commission (INEC) and others during the February 25, 2023 Presidential and National Assembly elections from within and outside Nigeria. Minister of Communications and Digital Economy, Prof. Isa Pantami, who made the disclosure, however, said the committee, set up and chaired by board chairman of Nigerian Communications Commission (NCC), with Chief Executive Officers (CEOs) of NCC, National Information Technology Development Agency (NITDA) and Galaxy Backbone Bone (GBB) as members, successfully protected the cyberspace, blocked the attacks and/or escalated them to relevant institutions for appropriate action [16][21]. In a statement by his spokesperson, Uwa Suleiman, the minister said the committee swung into action on February 24, 2023 and finished its work on 28. “During this period, a series of hacking attempts was recorded, including Distributed Denial of Service (DDoS), email and IPS attacks, SSH Login Attempts, Brute force Injection attempts, Path Traversal, Detection Evasion and Forceful Browsing. “A total of 12,988,978 attacks were recorded, originating from both within and outside Nigeria. It is worth noting that the centres successfully blocked these attacks and/or escalated them to relevant institutions for appropriate action,” he said. According to him, it is worth noting that in

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

the run-up to this year's general elections, threat intelligence revealed an astronomical rise in cyber threats, explaining that threats to public websites and portals averaged 1,550,000 daily. He added that this skyrocketed to 6,997,277 on presidential election day [22].

Pantami, said: "As part of its mandate, the ministry is to ensure adequate protection of Nigeria's cyberspace to a level that citizens would have confidence in digital services. This mandate aligns with the goals and objectives of the National Digital Economy Policy and Strategy for a Digital Nigeria (NDEPS) [22]. "In line with this mandate and in our efforts at supporting the initiatives of securing the Nigerian cyberspace, the parastatals under the supervision of the ministry have established cybersecurity centres, namely National Information Technology's (NITDA) Computer Emergency Readiness and Response Team (CERRT), Nigerian Communications Commission's Computer Security Incident Response Team (CSIRT) and Galaxy Backbone's (GBB) Security Operations Centre (SOC). The professor of Cybersecurity admitted that the parastatals have played a crucial role in providing enabling environment for successful conduct of credible, free, fair and transparent elections [23]. "In line with this mandate and in our efforts at supporting the initiatives of securing the Nigerian cyberspace, the parastatals under the supervision of the ministry have established cybersecurity centres, namely National Information Technology's (NITDA) Computer Emergency Readiness and Response Team (CERRT), Nigerian Communications Commission's Computer Security Incident Response Team (CSIRT) and Galaxy Backbone's (GBB) Security Operations Centre (SOC)[16]. The professor of cybersecurity admitted that the parastatals have played a crucial role in providing enabling environment for successful conduct of credible, free, fair and transparent elections.

**External Forces**

The chairman of the Independent National Electoral Commission (INEC), Professor Mahmood Yakubu, has said there have been attempts to hack into the commission's computer system ahead of the 2023 general elections. Yakubu spoke on Thursday during the 2022 National Conference of the National Association of Judiciary Correspondents (NAJUC) in Abuja with the theme, '2023 General Elections; Judiciary and Sustainability of Nigeria's Democracy." The INEC chairman who was represented by the deputy director of ICT, Dr Lawrence Bayode, said the attacks were from different parts of the world and not just Nigeria [23]. "We were looking at the system yesterday and we were seeing that people were trying to come into the system from France but we also are putting some things in place. "You can't build a house and you will not put a door, window or burglary; we have done our best to ensure that our system is secured," Bayode said [23]. He said the surfaced vulnerabilities of the Bimodal Voter Registration System (BVAS), the INEC Result Viewing Portal (IReV) and the backend were well-secured to make it difficult to beat. Bayode reiterated that there would be no voting without the permanent voter cards (PVC) and accreditation as provided in Section 47(1) of the Electoral Act, 2022. In the keynote address, the Attorney General of the Federation and Minister of Justice, Abubakar Malami (SAN), who was represented by his media aide, Dr Umar Gwandu, commended the media for its role in sustaining Nigeria's democracy while charging voters to resist the urge to sell their votes [23].

## VI. TYPES OF CYBER ATTACKS

Attackers take advantages of vulnerabilities and unleash devastating attacks on networks and servers. These attacks are categorized as follow:

**Malware**: Malware can be described as a coordinated convergence of cyber and virtual threats of various kinds, and typically consists of Trojan and other similar viruses [6]. It can be illustrated as the systematically designed instruction code that usually comes up with the rogue intent to hack the confidential information in the immune set. Malwares typically appear in the virtual scenario coupled with the attachments containing malicious emails, and the consequent download of the attached links that herald vulnerability-related issues.

**Phishing attacks**: These attacks typically ask a foreign agent for a reliable metric of information. In addition, often it comes with a request to register in a given connection that was endowed with the previous attachment. On that topic, what can be seen as an efficient index of Virtual intrusion seems to be some of the attachments request personal and sensitive data. In the past few days, this program has developed into a more advanced and elegant version where it allows users to switch to a third interface and external intrusions allow them to steal the knowledge accessible from foreign servers and users [10]. So, managing their malicious intent has become really simple and useful for the hacker.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

**Password attacks:** Generally these kinds of attacks are characterized by the intruder's intent to break the user's enforced password by merely initiating access to the user's device. Generally, this kind of attacker doesn't add some kind of debauch instructions and malicious codes. In addition, it does not misuse any tools to achieve its goals. In this case, a specific program is typically implemented that violates the prey user's password in a stably guided manner. It normally breaks a user's system's enforced password. There are certain specific program-related applications which possess the ability to initiate brute force attack. This form of program is typically developed and commissioned to crack the target user's password.

**DoS Attacks:** Typically, this sort of assailants imparts vehemence to chaos the ideals of a specific Network. In background, the approach by which DoS attacks are inflicted is unique in application since the intruders transmit a deep volume of network signal [8][13]. This aids congestion network traffic by overloading this. These forms of threats are considerably the most common form of cyber threats as it indulges the user in overcoming the network blockage imposed by the virtual intruder and meanwhile the hacker uses multiple networks to gain access to the preserved information.

**Man-in-the-Middle (MITM) attacks**: The attackers are intending to impersonate the various end nodes within a common service interface and information sharing. These forms of attacks are typically defined and interpreted throughout the Banking sector and financial industries, and are likely to target the online transaction interface. Usually, such attacks earned it access via a non-illusive wireless access node [8].

**Malvertising:** In such an attack, the automated attacker pressures the user to compromise with the fixed workstations while adding multiple criminal intent instructions. This malice is likely to occur if the user is prompted to access any questionable advertising index. These were a common practice for potential intruders to upload questionable and malicious material into the celestial system to confuse users and contaminate their collection of information at the same time. Clicking on the infectious connection will move the user to a different third-party interface and grab the confidential text [9].

**Eavesdropping:** This can be proven as a virtual overhearing environment where the possible attacker is vulnerable to secretly listening to other private exchanges. This is usually practiced among a particular network's diverse and shared hosts. This is not the serious kind of virtual hazard and can be solved by following a few simple acts.

**Click jacking:** These kinds of assailants typically target the user's normally used virtual interface by simply using some celestial malicious instructions in the form of cryptic codes [11]. This process is generally described as a cheap trick from the website of the hacker that makes inexpensive use of tricks and makes the user Click the button with apprehension. To redirect the respective user to another web page, this button is further conditioned. This sort of intruder can also be described as the possible hijackers who are vulnerable to stealing any valuable information from the user's network.

## VII. STAGES OF CYBER-ATTACK

Aimed cyber-attacks have no specific pattern of intervention, and therefore there is no chain of events that is absolutely accurate. An assault may be a one-time incident that lasts for minutes, or a segment of ongoing intrusions that extend weeks or even years, taking into account several technological and individual vulnerabilities, like unpatched websites that involuntarily trigger malware downloads, code injection web servers or browsers that are susceptible to downloading malware-infested mail attachments [11]. Overall, contemplating a targeted phase cyber intrusion is helpful. The targeted attacks occur across several phases:

**Reconnaissance:** In the early phase of an attack, an attacker makes use of social manipulation and passivity, Email Phishing, developing a waterhole or perverting removable media to gather information and learn its meaning. The hacker resumes by searching for open-source government
or corporate content, scanning, gathering data about targeted networks, their operations, critical staff and targeted mail addresses [11]. To detect vulnerabilities those need to be exploited, the attacker(s) invest some time cataloguing everything they discover to obtain profound insight into what is currently being utilized against the security features of database and the learning system.

**Scanning:** The next step will proceed for the hacker to find a low entry point that allows network connectivity; this may be poor judgment, restricted device utilization, perception management victims, lack of security strategy or ignorance. The intruder stealthily combines with normal traffic if a network is infected within the network, making identification increasingly hard. The attacker then starts by covertly implementing their cyber tools to isolate weaknesses in the protection within critical network connections [7]. The tracking system will search the systems probing area, searching for weaknesses to generate a server elevation cyber graph. This move may be done via resources that can be found

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

conveniently across the network. Searching for weaknesses is typically a long process and, regardless of how big the network is, it can take months.

**Arbitrary code execution:** Malicious actors may remotely build unauthorized network adapters or configuration issues on your device to install malicious programs such as Remote Access Trojans (RAT), root kits, and insert keystroke authentication software to acquire credentials for higher authorized access on the network, and also get passwords that will allow them to access all areas of the device. The intruder begins expanding after obtaining a set of appropriate systems on the preservation of the impact.

**Access and Escalation**: Now as the hacker has attained unrestricted control of the target system, they may try to push for lateral expansion and establish a strong presence. Many attackers hide in the Network's darkest regions, and stay inactive as they try to come and go. Some will choose to buckle across the network and identify the important parts they are hunting for genuine to accomplish their goal, such as sensitive information, private information, property rights or computer communications mechanisms that degrade or disrupt network activity at will.

**Data Collection, Exfiltration, and Exploitation:** The reputation of the network has been greatly undermined by this point. Once intruders think they have gained safe access to the system, they can now alter or transfer confidential data to any spot they wish. The attackers may use or leak the stolen data with third parties or even the Internet for more targeted hackers [15]. The ultimate goal of their mission is achieved and it is typically too hard for the breached enterprise to defend itself by this time.

**Clean up**: Not all attackers take the final step, some merely detach, and unworried about the victim possibly finding out just what happened or choosing to leave underneath a calling card to make a fuss about their achievement. Highly qualified attackers attempt to remove any forensic evidence that suggests a violation in all network systems [14]. They can erase / overwrite documents, erase embedded data, clear log files, disable alarms, roll back up software upgrades, unplug backups or erase hard disks. They would do their utmost to mask or delete any signs that the accident has ever happened, making it appear as a code error left behind secret backdoors anywhere they want to go back to, or breaching the systems further.

## VIII. CONCLUSION

Across the world, the introduction of electoral technologies has attracted contestations and controversies driven mainly by its propensity to enhance election credibility and undermine public trust in elections at the same time especially when electoral technologies are compromised. Most importantly, electoral technologies ensure efficiency in election administration and limit human interference with the electoral process. As these technologies evolve, attempts to compromise them heighten as elections can be stolen, and voter choices upturned by compromised election officials with a click of a button. Technology tools may also be subjected to disruptive cyber-attacks. These issues amplify the essence of greater transparency by election management bodies to increase public trust and confidence in electoral technologies. Perception is everything in life. Introduction of BVAS and IReV into the framework for election results management has transformed the public perception of the accuracy and credibility of election results. It is one of the most significant innovations and reforms to Nigeria's electoral process. Therefore, to increase the trust quotient in the BVAS and IReV, INEC should fortify their electoral technologies against cyber-attacks. Proper orientation should be given to INEC staff as well as citizens on the use of new technologies and perhaps possible vulnerabilities that could come and their level of preparedness.

## IX. RECOMMENDATIONS

Reposing confidence in the BVAS and Electronic Transmission of Election Results, INEC must do everything possible to secure their systems**.** Knowing some cyber-security basics and putting them in practice will help INEC protect their network infrastructures and reduce the risk of cyber-attacks. INEC should take IREV technology very seriously as this part of electoral process is very important as evident in the last general elections in Nigeria. The electoral body should tap into the immense security benefits of building their system security around machine learning technology. Also proper awareness on the use and workability of new technologies should be given to the electorates so that they are aware of how it works and the perhaps the legitimacy of its introduction Therefore, to increase the trust quotient in the BVAS and IReV technologies, INEC should implement the following actions as a matter of urgency:

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 10, Issue 4, April 2023

i. **Updating software regularly**: This includes your apps, web browsers, and operating systems. Set updates to happen automatically
ii. **Secure your files:** Back up important files offline, on an external hard drive, or in the cloud. Also make sure you store your paper files securely.
iii. **Require passwords:** Use passwords for all laptops, tablets, and smartphones. Do not leave these devices unattended in public places.
iv. **Encrypt devices:** Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.
v. **Use multi-factor authentication:** Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password, like a temporary code on a smartphone or a key that's inserted into a computer.
vi. **Secure your router:** Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.
vii. **Use at least WPA2 encryption:** Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.
viii. **Require strong passwords:** A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters. Never reuse passwords and don't share them on the phone, in texts, or by email. Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.
ix. **Train all staff:** Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.
x. **Have a plan:** Have a plan for saving data, running the systems, and notifying users if you experience a breach.

On the case BVAS, INEC is expected to do the following amendments in order to maximize the benefits of the new technology and improve efficiency.

i. There is need for BVAS Software Optimization
ii. Electronically transmit and publish voter accreditation data on the IReV
iii. Upload and transmit the ward collation results (Form EC8B) on the IReV
iv. Increase the processing power of the IReV
v. Timely conduct of penetration tests and mock exercises.
vi. Adopt a new approach to the training of election officials on electoral technology.
vii. Introduce official forms for reporting the cancellation of results at the polling unit

## REFERENCES

[1] Ajiji, Y. M. (2017). "Cybersecurity Issues in Nigeria and Challenges." International Journal of Advanced Research in Computer Science and Software Engineering 7(4): 315–321.
[2] Alkali, R. A. (2010). Issues in Nigerian Foreign Policy and International Relations. Kaduna, Nigeria: Media Press.
[3] Hoque, Sazzadul Mukit, A. Naser, A. (2012). An Implementation of Intrusion Detection System using Genetic Algorithm. International Journal of Network Security & Its Applications, 4(2), 109–120. https://doi.org/10.5121/ijnsa.2012.4208
[4] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4 PART 2), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066
[5] Borkar, A., Donode, A., & Kumari, A. (2018). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). Proceedings of the International
Conference on Inventive Computing and Informatics, ICICI 2017, Icici, 949–953. https://doi.org/10.1109/ICICI.2017.8365277.
[6] Akin, G., Bük, O., & Uçar, E. (2020). An inter-domain attack mitigating solution. Turkish Journal of Electrical Engineering and Computer Sciences, 28(2), 757–772. https://doi.org/10.3906/elk- Electronic copy available at: https://ssrn.com/abstract=3674442 International Journal of Case Studies in Business, IT, and Education (IJCSBE), ISSN: 2581-6942, Vol. 4, No. 2, August 2020.
[7] Z hang, Ningxia Yuan, Y. (2012). Phishing Detection Using Neural Network. CS229. https://doi.org/10.19026/rjit.6.2164
[8] Kato, K. & Klyuev, V. (2014). An Intelligent DDoS Attack Detection System Using Packet
Analysis and Support Vector Machine. International Journal of Intelligent Computing Research,
5(3), 464–471. https://doi.org/10.20533/ijicr.2042.4655.2014.0060
[9] Islam, R., & Abawajy, J. (2013). Multi-tier phishing detection and filtering approach. Journal of Network and Computer Applications, 36(1), 324–335. https://doi.org/10.1016/j.jnca.2012.05.009
[10] Zhang, Ningxia Yuan, Y. (2012). Phishing Detection Using Neural Network. CS229.
https://doi.org/10.19026/rjit.6.2164

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 10, Issue 4, April 2023

[11] Smadi, S., Aslam, N., Zhang, L., Alasem, R., & Hossain, M. A. (2015, December). Detection of phishing emails using data mining algorithms. In 2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA) (pp. 1-8). IEEE.
[12] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. Expert Systems with Applications, 37(12), 7913– 7921. https://doi.org/10.1016/j.eswa.2010.04.044
[13] Zhong, R., & Yue, G. (2010). DDoS Detection System Based on Data Mining. Proceedings of the Second International Symposium on Networking and Network Security, 1, 062–065. http://academypublisher.com/proc/isnns10/papers/isnns10p62.pdf
[14] Seissa, I. G., Ibrahim, J. & Yahaya, N. (2017). Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review. International Journal of Science and Research (IJSR), 6(1), 180–186. https://doi.org/10.21275/art20163936
[15] Zahid, M., Inayat, I., Daneva, M. & Mehmood, Z. (2020). A security risk mitigation framework for cyber physical systems. Journal of Software: Evolution and Process, 32(2), 1–15.
https://doi.org/10.1002/smr.2219
[16]https://guardian.ng/news/ministry-monitors-cyberspace-claims-inec-others-witness-12-9m-attacks
[17] https://www.vanguardngr.com/2023/02/voting-guide-to-nigerians-how-bvas-works/
[18] https://techcabal.com/2023/02/24/how-to-check-election-result/
[19]https://www.idea.int/news-media/news/inspiring-confidence-bvas-and-electronic-transmission-election-results-seven-urgent
[20] https://www.vanguardngr.com/2023/02/voting-guide-to-nigerians-how-bvas-works/
[21] https://techcabal.com/2023/02/24/how-to-check-election-result/
[22]https://guardian.ng/news/ministry-monitors-cyberspace-claims-inec-others-witness-12-9m-attacks/
[23] https://dailytrust.com/2023-foreign-hackers-attacking-our-database-inec-chair/
[24]https://www.reuters.com/world/europe/italy-sounds-alarm-large-scale-computer-hacking-attack-2023-02-05/
[25]https://www.serachdatacenter.techtarget.com/top-web.server-management-best-practices-and-essential-features
[26]https://www.serachdatacenter.techtarget.com/answer/how-does-a-web-server-model-different-from-an-application-server-model
[27]https://www.serachdatacenter.techtarget.com/feature/learn-the-major-types-of-server-hardware-and-their-pros-and-cons