ISSN No:-2456-2165

Exploring the Steps Taken by an Organization in Managing Data Security and Confidentiality for Availability and Integrity in a Case Study of an AOS Data Center in Rwanda

Dr. Musoni Wilson[1] Ph.D., Mupenzi Damian[2] Masters,
[1] Information Communication and Technology (ICT), University of Kigali, Kigali, Rwanda.
Subject area: Managing data security

Abstract:- This article focuses on how to revolutionize ICT in Rwanda, this study examined how security, data, and confidentiality are managed. As a case study, it will look at the actions done by the AOS data centre in Rwanda. To accomplish this, the study will define the various management roles for security, data, and confidentiality; investigate the actions taken by an organization, and assess the quality of information output produced by secure storage of data while it is being analyzed. It is also crucial to adhere to these practices. The government institutions data and personal information but don't establish a national data protection authority.

The security of confidential data and information belonging to the institution is of utmost importance. To guard against unapproved access to or publication of this information, the Information Technology (IT) Data centre AOS in Rwanda was established. The data center has taken many steps to reduce the danger of unauthorized access in order to guarantee this. As a result, the data center is determined to put into place rules and procedures that secure the acceptance, collection, storage, and eventual destruction of this data. These requirements may be federal, state, or other, including institutional policies. The use of R programming for data analysis and the statistical data management system gives insight into the management and analysis of quantitative data. The open-source R programming language has several tools for managing and analyzing quantitative data. This was confirmed by experiments utilizing the hacking tools Nmap and IP scan, which were employed by hackers to search for open ports on computers and network devices. The results of python or R programming show that there is a rather significant and favorable association between the development of technology and the efficacy of R programming. Additionally, research revealed that putting technology into practice has a favorable and significant impact on managing data security on Nmap's effectiveness. The top four features of Web Application Firewall (WAF) solutions that have a positive impact on user satisfaction are "Security monitoring," "Traffic Controls," and "Performance and Reliability." An algorithm selects these factors based on the traits in this category that are most likely to predict consumer satisfaction.

I. INTRODUCTION

In the contemporary digital era, protecting one's right to privacy is of the utmost significance. Data protection tries to do just that. Since the global economy is a digital economy and primarily depends on digitalization to leverage its economic success, this is especially crucial. Since the right to privacy is at the core of data protection, only a thorough understanding of the right to privacy can ensure that data protection in the digital era is adequately protected. The concept of privacy has evolved over time to mean numerous things**.**

The way in which privacy is protected by law at the national, regional, and international levels has surely changed as a consequence of the development of technology since our forefathers' time. By examining the community law in both jurisdictions, this essay seeks to provide a clear understanding, contrasts, and comparisons of the enforcement of data protection in Rwanda. The most progressive state in the EAC in terms of all data protection issues, Rwanda, will also be included in this paper as an example of some good practices.

According to statistics relating to the investigating procedures made by enterprises on managing data security and confidentiality for availability and integrity, there is a global problem with cyberattacks. Data protection is a big responsibility for organizations nowadays. Whether a data breach affects internal proprietary information or any type of customer data gathered, businesses may experience severe consequences. In order to protect against insider threats and cyberattacks, as well as to provide document security and guarantee data availability at all times, they must have the proper security policies in place. The information security policy of a company often focuses on these information security fundamentals. This idea also offers chances and strategies for safeguarding this information and data in both physical and virtual as well as online forms. The steps for doing this study are as follows: Information security (IS) definition, components, data security model, wearable technology, information security problem, and IS characteristics.

ISSN No:-2456-2165

II. METHODOLOGY

A. Data Analysis Methods

The computer systems design and related services industry includes AOS LTD, which is based in Kigali, Rwanda. At this facility, AOS LTD employs 72 people and generates sales of $7.97 million (USD). (The number of employees is guessed. This AOS Company is made up of businesses whose main business is to provide information technology expertise through one or more of the following activities.

- Creating, updating, testing, and maintaining software to satisfy the requirements of a specific client;
- Organizing and constructing computer systems that combine communication, computer hardware, and software technologies;
- Managing and running computer systems and/or data processing facilities for clients on-site;
- Expert guidance and services in computer-related fields.

The qualitative data from the interview guidelines were analyzed using thematic analysis. In order to explore the relationship between the predictor variable and either the independent variables and the criterion variable or the dependent variable, a prediction research approach was used in this study. Each participant in the sample provided two or more scores, one for each variable. This research methodology will be appropriate for and pertinent to our study because it required the researcher to gather information based on the current state of managing security, data, and confidentiality and to examine the actions taken by an organization in the case of the AOS data center in Rwanda. The findings were presented using narratives.

Data acquired through questionnaires were coded and evaluated using Kali, Nmap, and sophisticated IP scan software. Descriptive statistics including percentage, mean, and standard deviation were generated to describe the characteristics of the variables examined.

This study will examine the variables using Manage Engine Analytics Plus, IP scanner, Nmap, Wireshark, and R Data Analytics.

The NS3 (Network Simulator 3) and OP Manager will be utilized to deploy the suggested technique, and various metrics are employed to analyze the results.

B. Kali Nmap

Network Mapper is referred to as Nmap. Nmap in Kali Linux refers to a tool used commonly by penetration testers for system security evaluations and network discovery.

C. Response Rate for the Questionnaire and Interview Guide

This is the outcome of the respondents working together to communicate their thoughts on a specific question, which is expressed in several topics. 190 participants were sought for the study. Three interviewing guides and 190 questionnaires were successfully gathered by the researcher. A return rate of more than 50% is regarded as appropriate for study. This suggested that the data that had been gathered was adequate to carry out the analysis.

Additionally, data about respondents' experiences were gathered. The researcher wanted to gauge how the AOS data centre’s experience could affect how they integrated ICT tools into their experience-process. The following table provides a summary of the data collected:

Investigate elements do you think will affect how your organization manages data security and confidentiality, according to the responses provided to the questionnaire. One of the customer institutions and their general clientele at the AOS Data Centre, which made up half of the sample size, answered.

Examine the infrastructure your organization has in place for managing data security policies, as well as how it handles data security and confidentiality.

ISSN No:-2456-2165

	Variable	Number	Kolmogorov_Smirnova	Shapiro_Wilk	Jarquer_bera
0	Gender	95	0.434	0.586	2.23132
1	Position	95	0.234	0.827	1.23432
2	Education_Levele	95	0.294	0.783	2.00000
3	Academic_Qualification	95	0.333	0.802	5.80200
4	MDSAC:A1	95	0.242	0.820	1.82000
5	MDSAC:A2	95	0.299	0.678	3.57800
6	MDSAC:A3	95	0.270	0.769	3.46900
7	MDSAC:A4	95	0.283	0.786	1.76700
8	MDSAC:A5	95	0.317	0.780	2.78400
9	MDSAC:A6	95	0.264	0.780	1.78600
10	MDSAC:A7	95	0.303	0.765	1.66500
11	MDSAC:A8	95	0.263	0.792	5.79400
12	MDSAC:A9	95	0.293	0.756	5.75500
13	IFMDSP:B1	95	0.284	0.670	2.16700
14	IFMDSP:B2	95	0.312	0.677	1.57700
15	IFMDSP:B3	95	0.233	0.819	1.41900
16	IFMDSP:B4	95	0.262	0.785	3.79900
17	IFMDSP:B5	95	0.288	0.769	3.67900
18	IFMDSP:B6	95	0.309	0.685	3.58500
19	IFMDSP:B7	95	0.324	0.723	3.42300

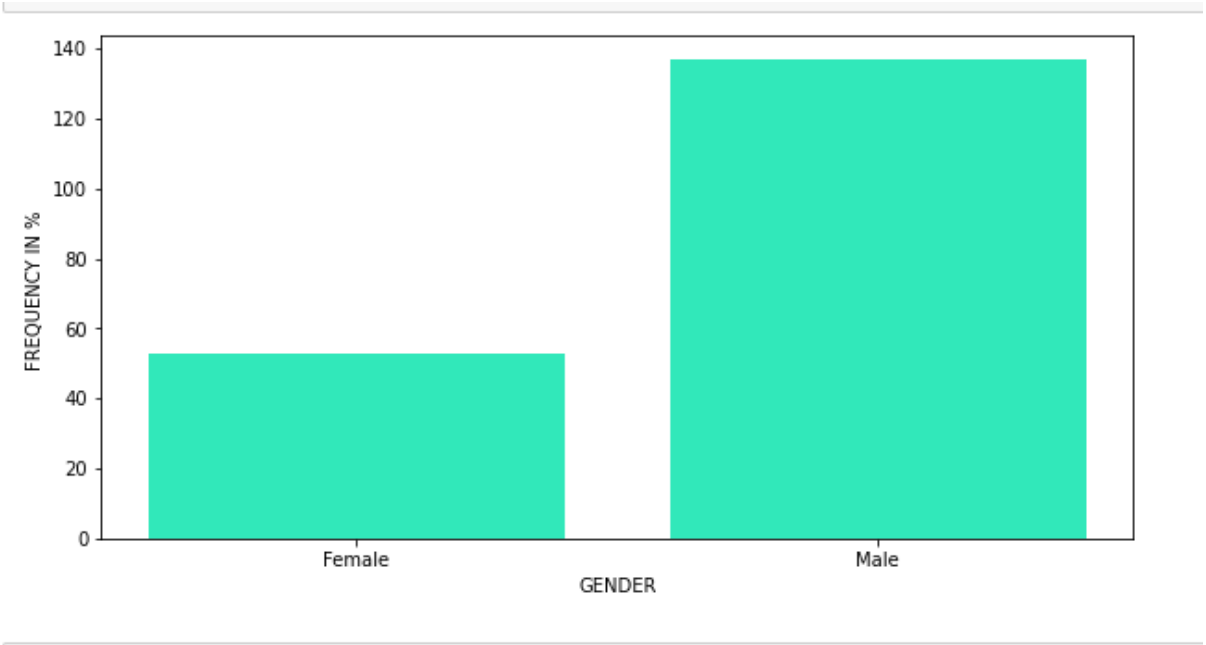
Fig. 1: Sample data set of questionnaire

III. DATA VISUALIZATION

The results that men made up 72.1% of respondents while women made up 27.9%. For the AOS data center in Rwanda to handle data security and confidentiality for the partners with government institutions and the country's business sectors, it is equally necessary for men and women, based on the facts mentioned above. This information comprises specifics regarding Bank of Kigali clients, AOS Data Centre partners, and AOS Data Centre customers in order to supply us with the results of respondents.

```
 #   Column              Non-Null Count  Dtype
---  ------              --------------  -----
 0   Status              3 non-null      object
 1   Gender              3 non-null      object
 2   Frequency           3 non-null      float64
 3   Percent             3 non-null      float64
 4   Valid Percent       3 non-null      float64
 5   Cumulative Percent  3 non-null      float64
```

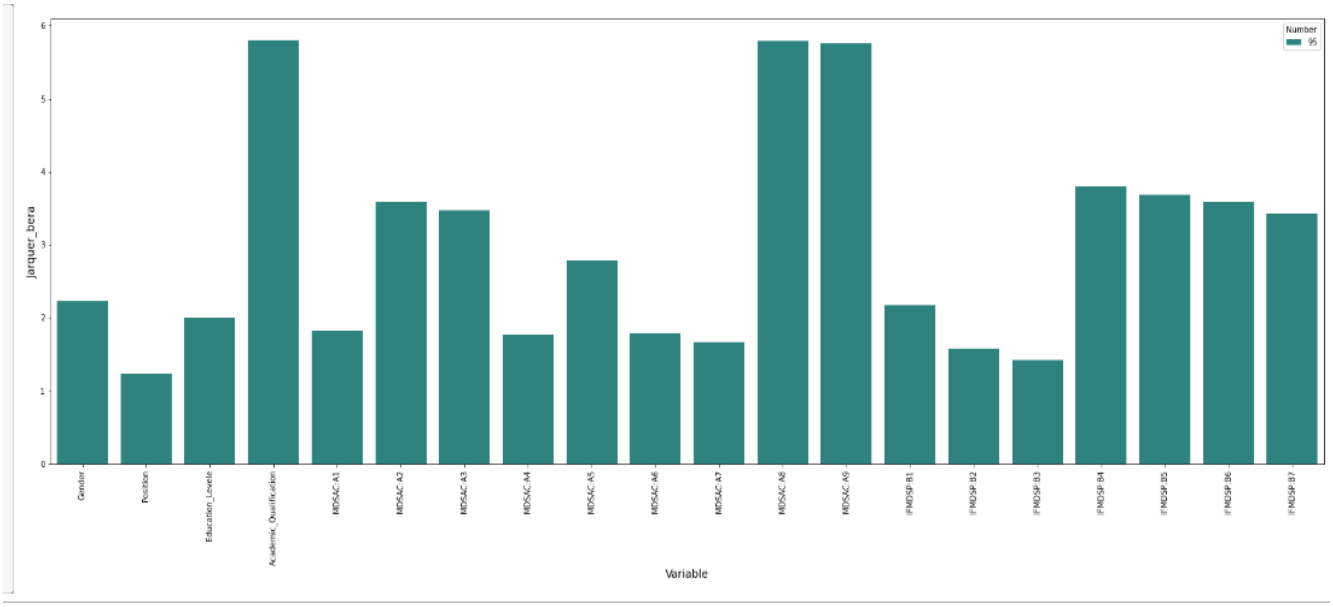
ISSN No:-2456-2165



Graph 1: Frequency Distribution by Percentage

It is simplest to import data into R as.csv files or python when using Excel to organize the data. However, data can be computerized using other applications, and R can read data that has been saved using such applications. With spaces separating the entries in each line of data, data stored as a text file (with a.txt extension) through Microsoft Word or other programs can be read using the read. Similar to Excel files, the data set should be organized with columns for variables and rows for subjects, with variable names ideally appearing in the first row of the document.

A fairly effective method to automatically distinguish samples from various distributions is the KS Test. To determine whether the provided data follows the Normal Distribution or not, use the kstest function. It contrasts the cumulative relative frequencies of the Normal Distribution as expected and as observed. The maximum absolute difference between the actual and anticipated cumulative distribution is used in the Kolmogorov-Smirnov test. The assumption of normalcy is the most often used assumptions test. The majority of parametric tests demand that the assumption of normality be satisfied. The distribution of the test is said to be normalized under the concept of normality. The following measurements and tests have been used to challenge the notion that everything is normal. The inquiry was created to address the issue with AOS data centers on data gathering. MANAGES DATA SECURITY AND CONFIDENTIALITY? (MDSAC) and INFRASTRUCTURE FOR MANAGING DATA SECURITY POLICY (IFMDSP)?



Graph 2: Existence of Response

ISSN No:-2456-2165

The Shapiro-Wilk test, a frequentist statistician's test for normalcy and which measures the normality of a distribution, can support our hypothesis.

Skewness should fall within the range of 2 to test the normal distribution hypothesis. Kurtosis levels should fall between 0 and 7.

W test by Shapiro-Wilk: The majority of academics employ this test to challenge the notion of normality. To satisfy the assumption of normalcy, Wilk's test shouldn't be statistically significant.

Test of Kolmogorov-Smirnov Most researchers employ the K-S test to verify the assumption of normality in the case of a sizable sample. This test should not be significant in order to satisfy the normalcy assumption.

Examine the infrastructure your organization has in place for managing data security policies, as well as how it handles data security and confidentiality.

A. Model denying penetration testing

Network Security Diagram

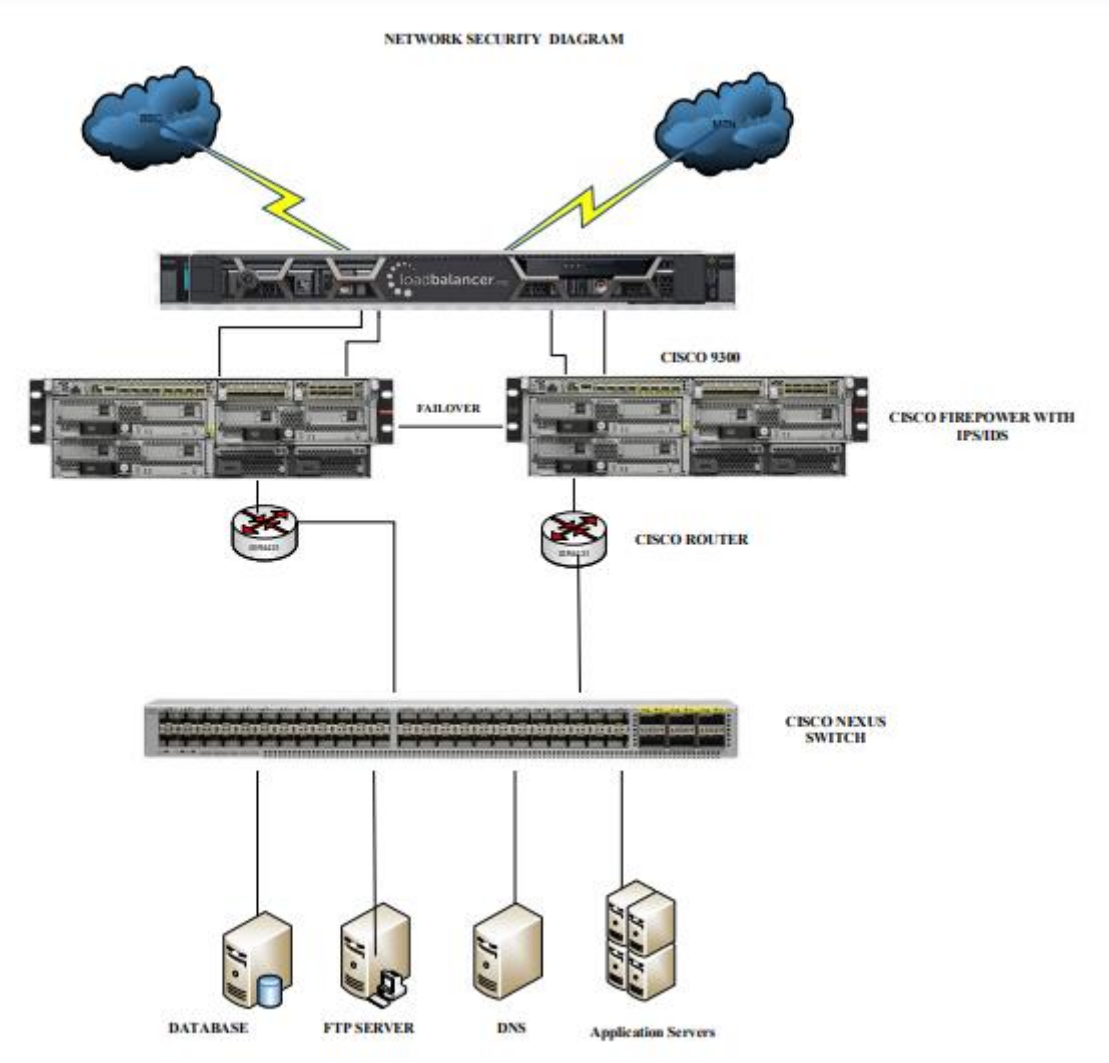


Fig. 2: Network Security Diagram

- **CLOUD INFRASTRUCTURE AND SECURITY ISSUES**

Fig. 2. harmful code attacks, DDoS attacks, network eavesdropping, etc. from the outside. The platform for cloud computing has three layers. Each physical machine in the infrastructure layer has several installed virtual machines (VMs). Customers can access the platform through the platform layer. users may install their own software, apps, and customizations. Additionally, the cloud providers' software stacks are provided through the software layer.

Customers on the client side could open-source legitimate users or attackers posing as legitimate users. Another option for man-in-the-middle attacks is for network eavesdroppers to occupy the middle positions. To secure the whole cloud environment, firewalls or intrusion detection systems (IDS) could be added.

ISSN No:-2456-2165

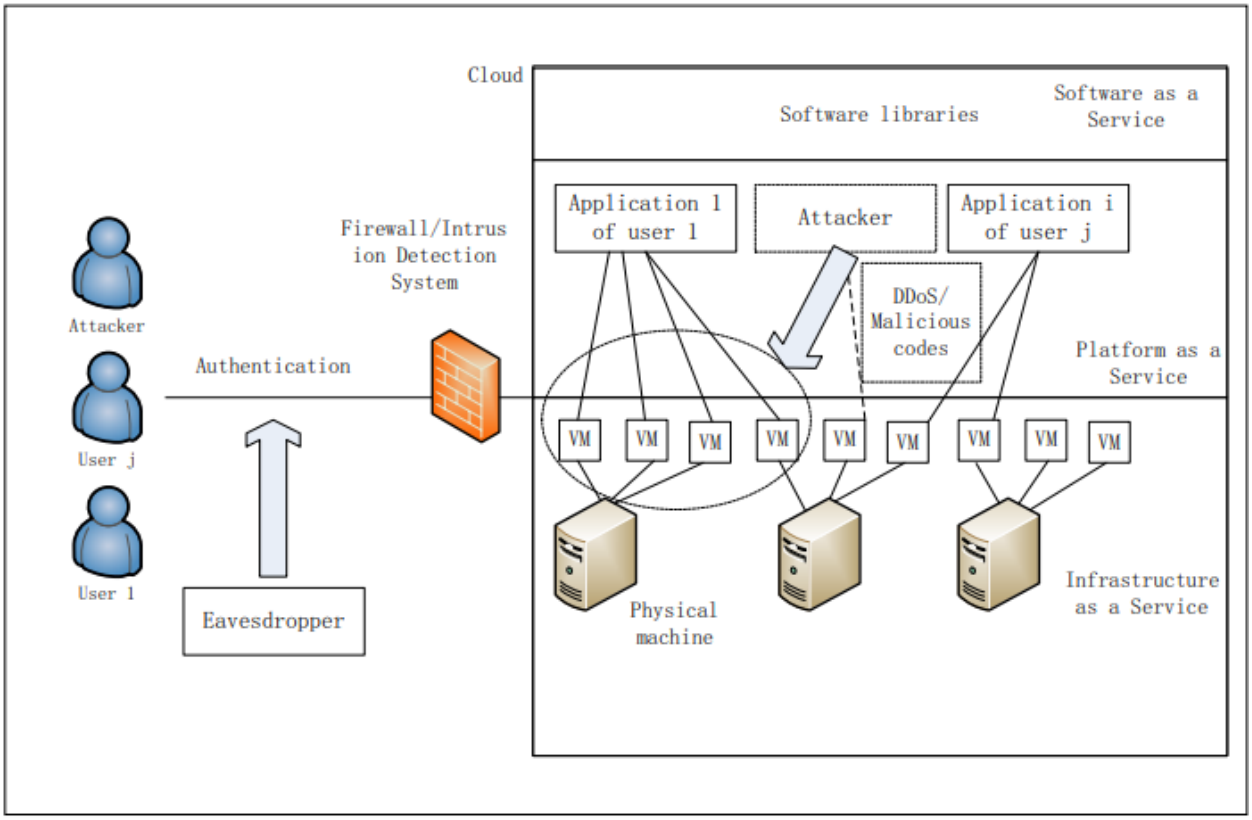


Fig. 3: Cloud Infrastructure and suspicious attacks

- **ISSUES WITH CLOUD DATA SECURITY**
  According to the analysis of cloud infrastructure and network security in AOS data centers, there may still be some vulnerabilities to cyberattacks that require attackers to be denied access to access points that can validate the weaknesses in the system of the AOS data center in Rwanda.

- **DATA STORED**
  A good enough AOS data center upgrade system with a solid foundation of Virtue Private network, load balancing, firewall, network access control, and intrusion detection systems/intrusion prevention systems, but my analysis requires a web application firewall in light of the data storage in their system, which keeps all data from public institutions and private sectors.

  ➢ Models for System Analysis
  The factors in this study were investigated using R, Python Data Analytics, and Manage Engine Analytics Plus.

  Advanced IP Scanner, NMAP, Wireshark, and Kali Linux for penetration testing and DB defense Demonstration of Kali Nmap for penetration testing.

  ➢ Results of Kali Nmap's model testing
  More than any other tool for penetration testing, Nmap is a port scanner. But by highlighting the ideal spots to attack, it helps pen testing. That helps ethical hackers identify network vulnerabilities. It is also free because it is open source. That makes it practical for individuals who are familiar with the open-source community, but it can be difficult for someone who is unfamiliar with such apps. Despite running on all major OSes, Linux users will find it to be more comfortable.

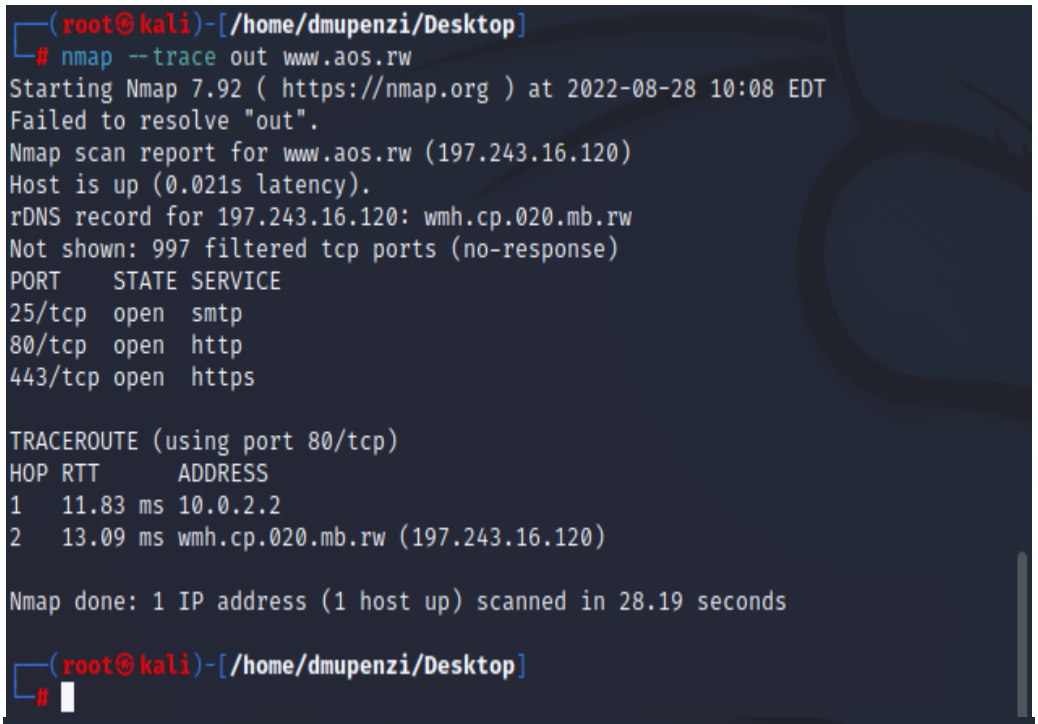
  This free network scanner is capable of everything, including host finding, port probing, and OS detection. The Nmap Scripting Engine can be used by anyone to create extensions, making it entirely extendable.

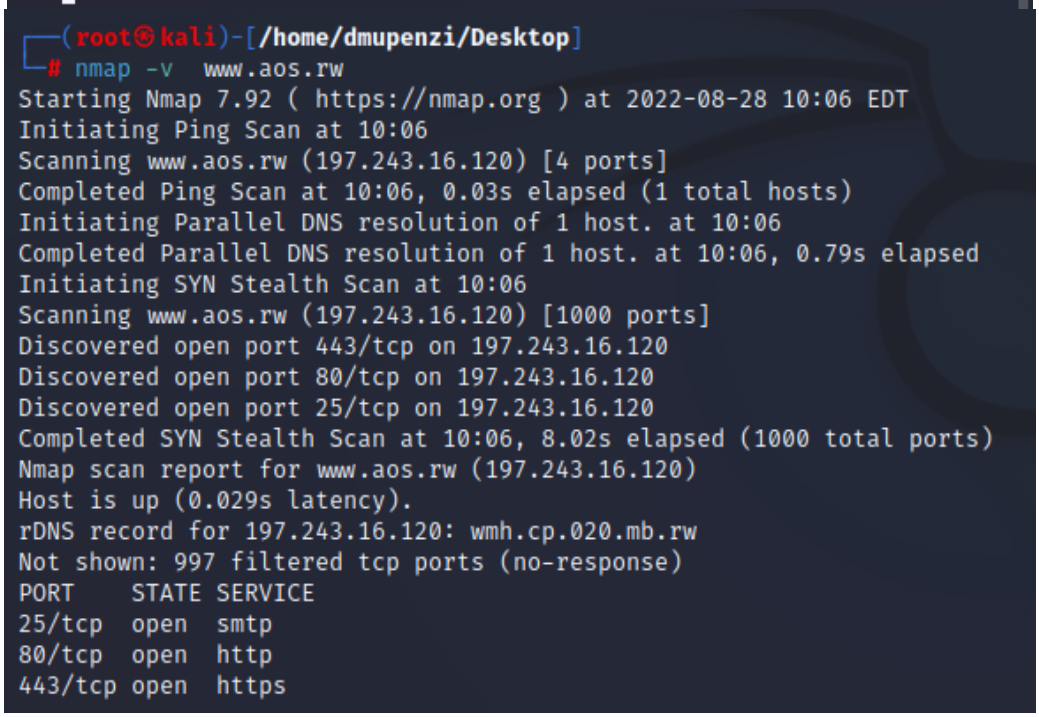
  The AOS domain name, www.aos.rw, pinging the Nmap system revealed open ports that pose a major risk to the company and its clients, especially the businesses and government organizations that collaborate with an organization at the AOS data center. The analysis of the essential components of the security policy utilizing a trustworthy model led to the discovery of open ports.

  The AOS data center had 1000 ports, some of which were open, according to the Nmap scanner. These open ports included 433/TCP, 25/TCP, and 80/TCP on 197.243.26.120, which exposes the company to risk and makes it possible for hackers to access their services as well as customers' services using the organization's ports.

  In contrast to other government institutions that are safe and have locked services and ports that cannot be readily hacked or granted access, their access points allow cyberattacks to infiltrate the system.

ISSN No:-2456-2165





Despite being a scanner, Nmap doesn't look for vulnerabilities, instead starting with human login credentials and moving on to their devices. It should be viewed more as an assessment tool to determine whether ports are open and which services are operational. There are certain scripts for vulnerability detection available.

This was confirmed by experiments utilizing the hacki ng tools Nmap and IP scan, which were employed by hacker s to search for open ports on computers and network device.

The results of python or R programming show that the re is a rather significant and favorable association between t he development of technology and the efficacy of R progra mming.

Additionally, studies revealed that putting technology i nto practice has a favorable and significant impact on manag ing data security and Nmap's effectiveness.

The Nmap displays all FIREWALL specifications, and because of this, it runs the danger of creating network problems that allow intruders, hackers, or other criminals to assault the data in the AOS data center. This dependable and lasting partnership has developed into a solid agreement to work together to accomplish greater objectives, including growing the ICT sector into a thriving industry, establishing Rwanda as the regional ICT hub, and promoting economic growth by enabling effective business service delivery in Rwanda and maintaining all data of government and institutional institutions.

ISSN No:-2456-2165

- DB defense model testing
  DB Defence is a simple, inexpensive, and efficient security solution for MS SQL Server that encrypts entire databases and safeguards their schema. It enables developers and database managers to fully encrypt databases. The database is shielded from unauthorized access, alteration, and distribution by Db Defence. It offers a broad and robust selection of database security capabilities, including powerful encryption and SQL protection from SQL Profiler.

  Since databases are the core of any organization, it is imperative that they be protected at all costs. When an attacker has access to the database, they might expose it and damage it, disrupting the organization's operations as a whole. However, by using and testing our databases with these technologies, we can ensure the security of the database. There are other additional tools accessible as well, but these are some of the ones that knowledgeable experts from the AOS data center in Rwanda most frequently advise using.

  The respondents made note of how technology has increased crime surveillance and monitoring, making it simpler to spot and eradicate crime. To further guarantee data security and confidentiality, load balancing, a key networking method used to disperse traffic over several servers in a server farm, as well as firewalls and other network devices that are encrypted, are used.

IV. CONCLUSION

Analyzing how to manage data security and privacy: Investigate the actions made by a company, case study the objective of this investigation was to the AOS data center in Rwanda. This study produced a wide range of conclusions, starting with the demographic findings. According to the study, the majority of participants—including some AOS data center bank of Kigali personnel and the remaining customers—were men (72.9%), while 27.1% were women.

Additionally, data about the respondents' experiences were gathered. The researcher was curious to know how the AOS data center's expertise would affect how they integrated ICT tools into their experience process.

Investigate elements that, based on survey responses, you think will affect how your company manages data security and confidentiality. A customer institution and their general clients at the AOS Data Center made up half of the sample size, and they answered.

The AOS domain name, www.aos.rw, pinging the Nmap system revealed open ports that pose a major risk to the company and its clients, notably the businesses and government organizations that work with an organization at the AOS data centre.

The Nmap scanner discovered that the AOS data center had 1000 ports, some of which were open. On 197.243.26.120, there were open ports for 433/tcp, 25/tcp, and 80/tcp, putting the business at danger and making it easy for hackers to access both their services and those of their clients.

Network analysts and penetration testers can benefit from Nmap. By copying and pasting the printed information from the console into a text editor, one may perform the required analytics there. Kali Linux also provides a utility that enables you to store the complete Nmap scan findings to a file for later use. With just a single base command and a number of additional parameters, Nmap offers customers a lot of information to protect workstations against unauthorized intrusions.

V. RECOMMENDATION

In order to prevent problems with intruders or cyberattacks from affecting government institutions or other private sector businesses, the AOS data center should have its ports closed and its services configured. A web application firewall that keeps track of all activity brought on by intrusions should exist because of this.

The top four features of Web Application Firewall (WAF) solutions that have a positive impact on user satisfaction are "Security monitoring," "Traffic Controls," and "Performance and Reliability." The features in this category that are most likely to predict customer satisfaction are chosen by an algorithm to create these variables.

A firewall called a web application firewall keeps track of, filters, and blocks data packets traveling to and from a website or online application (WAF). The AOS data center in Rwanda will advise employing a web application firewall to manage data security and confidentiality at an organization due to the requirement to secure the data of partners in the public and private sectors. A WAF is often installed through a reverse proxy and then put in front of one or more websites or apps. It could be host-, network-, or cloud-based. The WAF uses a rule base that it applies to every packet to investigate the Layer 7 web application logic in order to find potentially dangerous traffic that could assist web assaults.

- The future researchers
  - Future researchers ought to check the open ports of the AOS data center to make sure that the organizations that store data there are unaffected and to determine whether their ports have been exploited by outsiders accessing their services
  - Customer-focused algorithms must be created because algorithms are used over encrypted data. Users must be well-versed in encrypted data.
  - It is necessary to plan, execute, and assess a fully working system benchmark using both quantitative and qualitative performance measures.
  - It is crucial to note that this study has some limitations even though it has provided a complete overview of the actions performed by the AOS data center in Rwanda to manage data security and confidentiality.

The findings are difficult to generalize because they were based on a small sample of participant experiences and opinions. In order to ensure that an appropriate security strategy is developed and implemented throughout the entire company, additional studies on an expanded analyze who is in charge of securing critical data. Projects like the Rwanda AOS Data Center were required. Researchers should look for emerging technologies that can enhance and evaluate management information systems in order to safeguard an organization's information system (MIS).

REFERENCES

[1.] Malcolm W. Harkins, (2014). W. Harkins, Managing Risk, and Information Security. DOI 10.1007/978-1-4842-1455-8_11.
[2.] 5020 Weston Parkway, Suite 200, Cary, North Carolina 27513. (2016). Data security policy. www.lawyersmutualnc.com
[3.] Montclaire state university. (2015). Responsible Use of University Computing Resources Policy Document Data Classification and Handling (Safeguarding Sensitive and Confidential Information).
[4.] Sandeep Dhawan. (2016). Information and Data Security Concepts, Integrations, Limitations and Future.
[5.] AOS transforming ICT in Africa, (2014), https://www.aos.rw/about/company-overview/,https://www.aos.rw/news/aos-ltd-celebrating-liberation-with-intensified-efforts-of-turning-rwanda-into-an-it-hub
[6.] Dr. Vijayalakshmi, (2021), Impacts of cybercrime on internet banking, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3939579
[7.] All Africa,(2021), https://allafrica.com/stories/202007300062.html
[8.] Ktpress,(2021),https://www.ktpress.rw/2021/10/2022-to-be-a-year-of-cyber-crimes-battle/
[9.] New times, (2022), Is the war on cyber-crime already yielding results?
[10.] https://www.newtimes.co.rw/news/war-cyber-crime
[11.] Mohammed Mahfouz Alhassan and Alexander Adjei-Quaye,(2017),Information in security an organization, (PDF) Information Security in an Organization (researchgate.net).
[12.] Wilbur L. Ross, Jr.,(2020), Security and Privacy Controlsfor Information Systems andOrganizations,https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[13.] Yue Shi, (2019), Data Security and Privacy Protection in Public Cloud.
[14.] Mikko T. Siponen and Harri Oinas-Kukkonen, (2015), a Review of Information Security Issues and Respective Research Contributions.
[15.] RISA, (2015), National Cyber Security Policy.
[16.] Ministry of Youth and ICT, (2017), National data Revolution policy, file:///C:/Users/hp/Downloads/Rwanda_Data_Revolution_Policy.pdf.
[17.] Shahzad, F., Pasha, M., & Ahmad A (2017), A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. International Journal of Computer Science and Information Security, Vol. 14, No. 12. arXiv preprint arXiv:1702.07136
[18.] Craig A. Horne, Atif Ahmad & Sean B. Maynard,(2017), A Theory on Information Security
[19.] Peter Schattner &Danielle Mozza(2006),doing pilot study,:
[20.] Yue Shi (2019), Protection of privacy and data in public clouds