Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Cyber Security Exploits and Management in Telecommunication Companies: The Case of Uganda

Washington Okori[1] ✉ and Sarah Buteraba[2]
[12]Computing for Development Limited, P.O. Box 928, Kampala, Uganda
Corresponding Author: Washington Okori, **E-mail**: gokori@gmail.com

| ABSTRACT
This study examined the risks faced by telecommunication companies due to cyber-attacks and threats to their critical information infrastructure. It suggests control measures to avert the vulnerabilities of such infrastructure to cyber attackers. Critical information infrastructure is important to the companies as a revenue enabler and reputation identifier. However, the infrastructure, if not well protected, can be a national security threat, affect the national economy, and disrupt societal integration and business globally. Cyber security is the protection of internet-connected systems, including hardware, software, people, and data, from cyber-attacks. Its threat exploits the increased complexity and connectivity of critical infrastructure systems. The identification of the critical information infrastructure was done through document analysis and discussion with the network technical teams. The infrastructure systems, such as devices, servers, data, database, firewall, and network, were identified in this study as vulnerable to attack. This study suggests a framework to support timely intrusion detection and for the protection of critical information infrastructure. To secure and safeguard the critical information infrastructure from inherent vulnerabilities, it is recommended that continuous monitoring of the critical infrastructure attack gates should be made part of the overall risk management of a telecommunication company, and innovations in cyber security detection and prevention should be harnessed.

| KEYWORDS

Cyber-attack, Cybersecurity, Infrastructure, Vulnerability.

| ARTICLE INFORMATION

ACCEPTED: 26 September 2024 **PUBLISHED:** 05 October 2024 **DOI:** 10.32996/jcsts.2024.6.4.10

1. Introduction

Cybercrime is among the most prevalent risks associated with advancements in digital technology in the world today (Ramadani *et al.,* 2018; Venkatachary *et al.*, 2018; Smith R.G., 2007). Cyberattacks are the third highest global risk, according to the World Economic Forum (WEF, 2018). The data revolution has witnessed increased interaction, complexity, and connectivity amongst different critical infrastructure systems, and therefore, it is necessary to implement appropriate security measures to prevent or minimize attacks and data breaches by cybercriminals. Since most of these systems are remotely reachable, strong cybersecurity measures should be implemented to protect them from cyber-attacks. The system components that need protection from attacks include, among others, computers, servers, mobile devices, and networks.

Telecommunication companies' networks progressed from circuit-switched based PSTN (Public Switched Telephone Network) networks as was in the 1G technology to the 4G with LTE (Long Term Evolution) standard, which is packet-switched and now to 5G. The purpose is to provide a high-speed data transmission rate and good voice quality to users with improved security and lower cost of voice and data services. The 4G next generation network and 5G can deliver voice, data, and multimedia service over the Internet Protocol (IP). However, IP-based systems are prone to security challenges such as cyberattacks since they use open protocol standards, as corroborated in documentation by the Ministry of Communication and Information Technology, India

(2012). This transition from the circuit to packet switched network has increased the vulnerability of the telecom networks. The 5G is expected to be one hundred times faster than 4G but will be more susceptible to cyber-attacks since it will support the Internet of Things (IoT), where almost everything in life will be connected for seamless efficiency.

With the improvement in data transfer speeds, secure and accurate information is a prerequisite in the telecommunication industry. With the advent of advances in technology, information technology (IT) needs of telecommunication companies have evolved and necessitated the addition of new capabilities and resources and increasing storage capacity at minimal costs. The use of cloud services has offered an opportunity to minimize costs related to licensing, infrastructure, and training. The major service models for cloud computing (Garrison *et al*., 2012) are (i) Software-as-a-Service (SaaS), where a third-party provider hosts applications such as Customer Relationship Management (CRM) and makes them available to customers over the Internet. The applications are accessible from any end user device, such as smartphones, via a web browser. (ii) Platform-as-a-Service (PaaS), where the client deploys custom applications onto the cloud infrastructure provided and supported by the service provider. (iii) Infrastructure-as-a-Service (IaaS) is a pay-as-you-go service for storage, networking, and virtualization. As stated by Buttell (2010), the user is capable of deploying and running proprietary software and Operating System (OS) for their own use. Cloud-based computing presents novel security threats due to the insecurities of APIs and various hardware vulnerabilities. Despite challenges such as continuous availability, chances of network disruption, data lock, and confidentiality, cyber security exploits also exist.

Currently, there is an increase in the use of smart devices such as smartphones and tablets. In these devices, logins, passwords, and other important information are stored. Emails, social media accounts, and other applications are easy to access when using such smart devices. Theft or loss of a device is an access point to sensitive corporate data. The devices, too, are easy targets for viruses such as trojans, worms, and spyware, which make it easy for attackers to gain access to proprietary data. Since these devices can be used to access corporate networks remotely, the attackers can deploy off-the-shelf malware to hack specific applications of interest. Telecommunication companies should, therefore, build strong safeguards against access to the database, applications, and network including devices such as routers and interception of data in transit.

This study is congruent with earlier theories, such as the Socio-technical System theory, which considered the interaction of human element in organizations with the surrounding technologies in seeking to understand how people search, obtain, evaluate, share, classify, and make use of the information provided by the information technology (Bostrom and Heinen, 1977, Zaini *et al*., 2018). Also, the information security theory considers the preservation of integrity, confidentiality, availability, and non-repudiation of information as basics of information security in an organization (Siponen and Oinas-Kukkonen 2007). Jang-Jaccard and Nepal (2014) observed that cyber-attacks and defense strategies should enforce confidentiality, integrity, and availability (CIA) of any digital and information technologies. This study considers additional elements such as critical infrastructure, attack motivations, control of unauthorized access to information, resources, and information sharing over the cloud, and people as constituents in the management of cyber security.

With the wide range of end-user devices that can now connect to telecom networks, the vulnerability and risks of attacks have increased. Telecom companies in different Operating Countries are focusing their efforts on preventing and responding to this increasing threat (GSMA, 2019). The extent of attacks, if not mitigated, can place the nation's security, economy, public safety, and health at risk. At the organizational level, it affects reputation, customer trust, and revenue. In this study, we define Cybersecurity as the protection of internet-connected systems, including hardware, software, people, and data, from cyberattacks.

This study aims to identify critical infrastructures of telecommunication operators in Uganda vulnerable to cyber-attacks, control measures to mitigate attacks on such critical infrastructure, and suggest a framework that can enhance timely intrusion detection of cyber-attacks.

The study attempts to answer the following research questions:

(i) What are the common motivations for cyber-attacks by cybercriminals?
(ii) What are the most critical infrastructures vulnerable to cyber-attacks by cybercriminals?
(iii) How can cyber-attacks on telecommunications critical infrastructures be detected?
(iv) How can intrusion detection of cyber-attacks be improved?

1.1. Cyber security challenge in digital business

In Uganda, telecommunication companies have embraced digital transformation that has significantly improved their business performance. The transformation has supported decision-making at the different levels of management and increased financial inclusion in the country. With Uganda's economy growing at approximately 6% per annum, the telecom sector is growing at 17.4% per year, providing one of the best gross revenue turnovers in the country. The total telecom subscribers increased by

157% over the last 10 years, from 10 million in 2009 to 25.7 million in 2019. The internet penetration increased by approximately 15 million, which represents 165% growth (UCC, 2019).

The Digital transformation has witnessed the introduction of mobile money services in Uganda. This service is more widely used than the banking system to make payments, and this has enabled greater financial access and use, as well as the facilitation of remittances and trade (Bank of Uganda, 2019). The mobile money platform, which is part of the critical telecommunication infrastructure, becomes a target for attack by fraudsters for financial gain. The attackers strive to gain access to the mobile money personal identification number (PIN) to enable them to withdraw money from the victims' mobile money account. The mobile money providers, therefore, should improve the overall security landscape of the mobile money services.

Decision-making at the operational and strategic levels has also seen the wider application of business intelligence (BI). In a competitive telecommunication environment like Uganda, where there is no monopoly, businesses need to analyze their key metrics in order to get insight into their business performance and customer experience at all levels. Telecommunication companies have employed BI tools such as Tableau and Power BI to do predictive analysis, data mining, forecasting, and provision of reporting dashboards. This is in addition to proprietary in-house developed BI tools. Big data analytics is another area where telecommunication companies are making the investment to take advantage of the available information within their networks to make them robust, optimized, and scalable by analyzing network traffic in real time. With the help of big data, telecom companies can analyze customer behavior, which supports the delivery of customer-tailored products, grow their customer base, and increase revenue. Messaging technologies have revolutionized how we communicate, with messaging apps such as WhatsApp, Facebook, and Twitter trending. Currently, media and entertainment streams are emerging in Uganda, and services such as internet television bypass cable and deliver video directly to viewers through a broadband connection.

With the emergence of this transformation, cyber attackers continue to want to gain access to the systems in a company in many ways, as argued by contributors like Lee (2008) as follows:

(i) Distributed Denial of Services (DDoS), which by agents generates sizable amounts of data packets, which may exhaust the computing and communication resources of a target in a very short duration.
(ii) Phishing is an attempt by scammers to trick victims into giving out personal information such as bank account numbers, passwords, and credit card numbers over media like emails.
(iii) Malware is a piece of software written with the intent of causing harm to data and devices.
(iv) Ransomware that attacks your computer network and encrypts files, denying access to the files. The attackers demand large sums of money to get your data back.
(v) The attackers gain access to an information technology system and use it as a launch pad for an assault on a more attractive target.

With the advancement in technology from circuit to packet-switched IP-based networks, there is increased vulnerability and risks of attacks. The availability of varied interfaces connecting to the network becomes susceptible to cyber-attacks. Telecom companies in different Operating countries are focusing their efforts on preventing and responding to this increasing threat. (GSMA, 2019).

To avert these threats, telecommunication companies constantly monitor their infrastructure to avoid cyberattacks. The tests that are majorly conducted include network scanning, where a port scanner identifies all the hosts connected to the network; vulnerability testing, ethical hacking, and password cracking; and penetration testing, which is an authorized simulated cyberattack. Technologies such as Dispersive Technologies that block Man-in-the-Middle (MiM) attacks are being developed. Man-in-the-Middle is a hijack attack in communication between two parties whilst eavesdropping and transmitting a message that will make them believe they are having authentic communication when it is an altered message. The attacker then takes control of the fraudulent communication (Keijo and Pekka, 2008)

2. Materials and Method

Qualitative research methodology was used (Conboy *et al*., 2012) since the study attempted to gain an understanding of underlying reasons, opinions, and motivations for using some of the technologies in cyber security.

The case study method (Yin, 2014) was adopted since the study dwelt on the cyber-attack and cyber-security aspects of the industry. The grounded theory method (Corbin and Strauss, 2008) supported the research since we reviewed documentation from journals and technical reports on topics related to cyber-attacks and cyber-security as managed in other telecommunication companies. The technical discussions covered tests such as network scanning, vulnerability scanning, password cracking, ethical hacking, and penetration tests, while documentation reviewed motivation for attacks and control measures.

3. Results

3.1 Common attack vectors and payload

The cyber attacker's goal is to gain unauthorized access to the critical information infrastructure or system with malicious intentions. The attackers exploit system vulnerabilities using various attack vectors with intended payloads, as indicated in Figure 1.

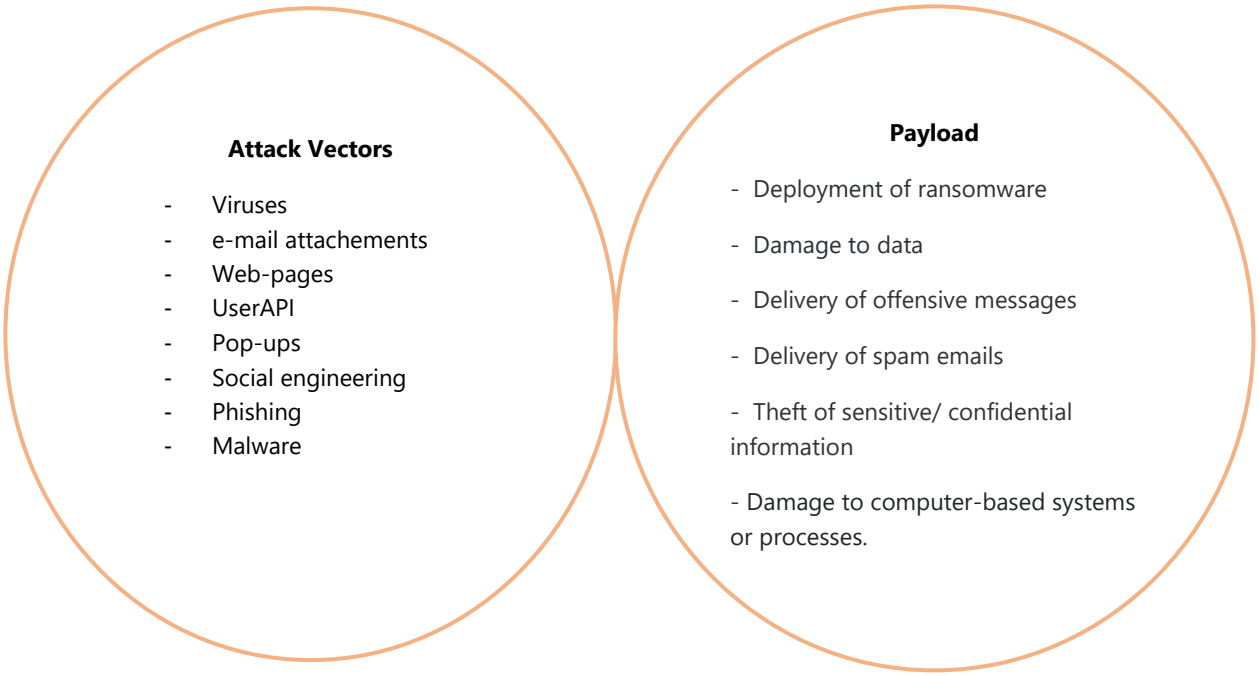

Figure 1: Common attack vectors and payload. Source: Author

3.2 Attack gates and defense mechanism

Vulnerability gates used by the attackers to gain entry into the systems to cause malicious damages were identified. These gates, if not well managed or protected, can be used as launch pads for attacks by cybercriminals. The attack gates and defense mechanisms for each gate are listed in Table 1

Table 1 Attack gates and defense mechanism to minimise access to systems.

Attack gates	Defense mechanism
Usernames and passwords	- Strict Password management policy - Use of biometrics
Disgruntled employees	- Close management of permissions and privileges to confidential information
Poor encryption standard	- Use of encryption methods like Secured Socket Layer (SSL) that can prevent attacks such as man-in-the-middle and protect the confidentiality of data being transmitted
Misconfiguration at the cloud, servers, routers, and switches	- Install firewall - Have filters on the router to prevent unauthorized users from logging or sending management traffic into the router. - Intelligent use of the action control list (ACL) to permit only specific source IP address and protocol. - Protect configuration files with encryption or access control when sending, storing, and backing up files. - Periodic test of security configurations against security requirements

Cookies	- Disable the storage of cookies in your internet browser through your browsers privacy setting. - Abandon website if requested to accept cookies you are not sure of its legitimacy. - Use browser add-ons to block third-party software such as cookie trackers and ensure that your browsing habits remain private. - Develop a capability of validation of data input by users in an HTTP request before reflecting it back as one of the safe guards to defend against cross-site scripting, which may expose details in the cookies to attackers.
Third party vendors/ platforms	- Continuously monitor changes in their security posture. - Ensure data security issues and expectations are formalized in the contract.
User API	- Perform penetration testing to check for exploitable vulnerabilities from both the API provider and developers.
Web browsers	- Use host-based intrusion detection systems that will monitor Web traffic to identify and stop malicious actions. - Send all traffic through a proxy - Use the most recent major release

The users' profiles should also be monitored by the systems administrators to ensure that all privileges are in synchronization with the defined roles in the organization. Some users may exploit the unwarranted privilege granted to them either by mistake or intentionally to commit fraud or abuse.

3.3 Critical infrastructure

The critical infrastructure to be secured by telecommunication companies from the attackers was identified with corresponding mitigation measures, as shown in Table 2.

Table 2 Critical infrastructure vulnerable to cyber attack

Critical Infrastructure	Mitigation against attack
Database servers	- Regular deployment of database patches - Regular Data back up - Access control - Change Advisory Board approval for any change in the database - Separation of test and production environment - Grant limited permissions in your databases to Avoid SQL injection attack
Application servers	- Regular deployment of database patches - Regular Data back up - Access control - Installation of anti virus such as Kaspersky to secure workstations and servers - Separation of test and production environment - Change Advisory Board approval for installation of new applications
Network Security servers	- Deployment of OS patches - Use of advance data encryption standards (DES) such as triple DES - Install firewall - Change Advisory Board approval for any changes

Mail server	- Host own email server. - In Simple Mail Transfer Protocol (SMTP) settings, limit number of simultaneous connections - Limit mail relay for SMTP server to only authenticated user email accounts - Ensure spam filter is activated - Ensure that the domain that your corporate email uses has at least two mail exchange (MX) records, with secondary and tertiary MX records, for necessary redundancy when the primary MX record fails. - Use Secure Socket Layer (SSL) options such as Internet Message Access Protocol (IMAP) and SMTP as standard TCP/IP ports.

The safeguarding of the critical infrastructure should be complemented with end-user training to enlighten employees about security awareness. The IT policy should be developed to include segregation of roles, incidence response plan, frequency of cyber risk assessment, security protocols, and procedures. The company should have a disaster recovery (DR) plan to provide continuous replication of critical applications, infrastructure, data, and systems for rapid recovery in case of an outage.

3.4 Security bubble framework

The study suggests a security bubble framework that can be adopted by telecommunication companies in the wake of an increase in cybercrimes (Figure 2). In this framework, the incorporation of a dynamic, intelligent detection monitor along the pathway from the cloud to the individual gates could minimize intrusion by attackers.

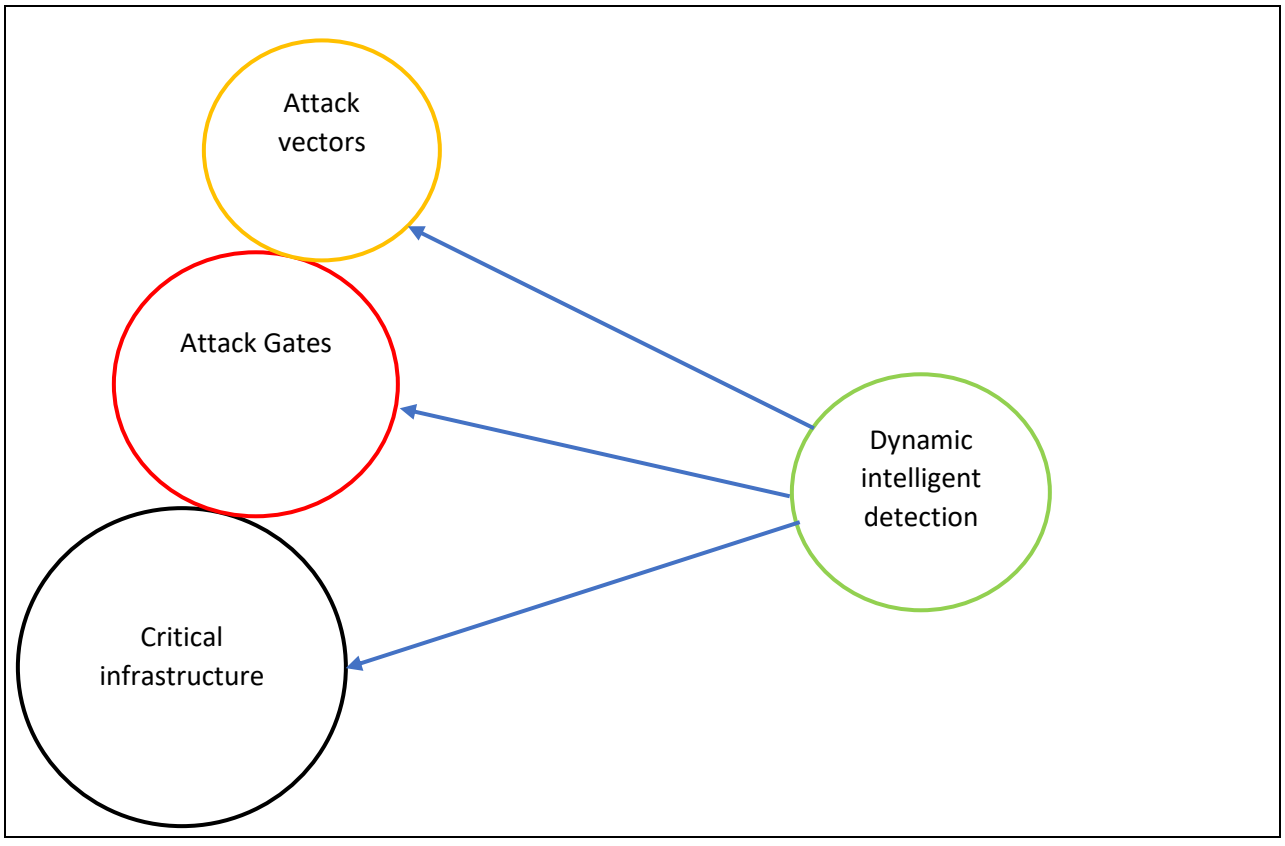

Figure 2 Security bubble framework. **Source: Author.**

3.5 Implementation and evaluation strategy

Continuous monitoring of activities in the network should support the implementation of dynamic, intelligent detection based on the security bubble framework. Monitoring and control of network traffic to and from the cloud with network infrastructure tools such as routers and firewalls reduces the extent of vulnerability in case of an attack. A firewall blocks malicious traffic requests and data packets while allowing the flow of legitimate traffic; however, if not properly configured or/and secured, it can be used to exploit the network. The network should be segmented based on roles and functions to ease monitoring of ongoing activities and

subsequent control in case an intruder infiltrates. A router can be used to separate the different segments. Within the same segment, create domains to isolate users further by groups for proper control and management. A domain or virtual local area network (VLAN) should contain a group of devices that communicate most frequently. A router can separate the different virtual local area networks. A virtual local area network access control list (VACL) should be maintained to control traffic flow between the different LANs. The proposed architecture is shown in Figure 3.

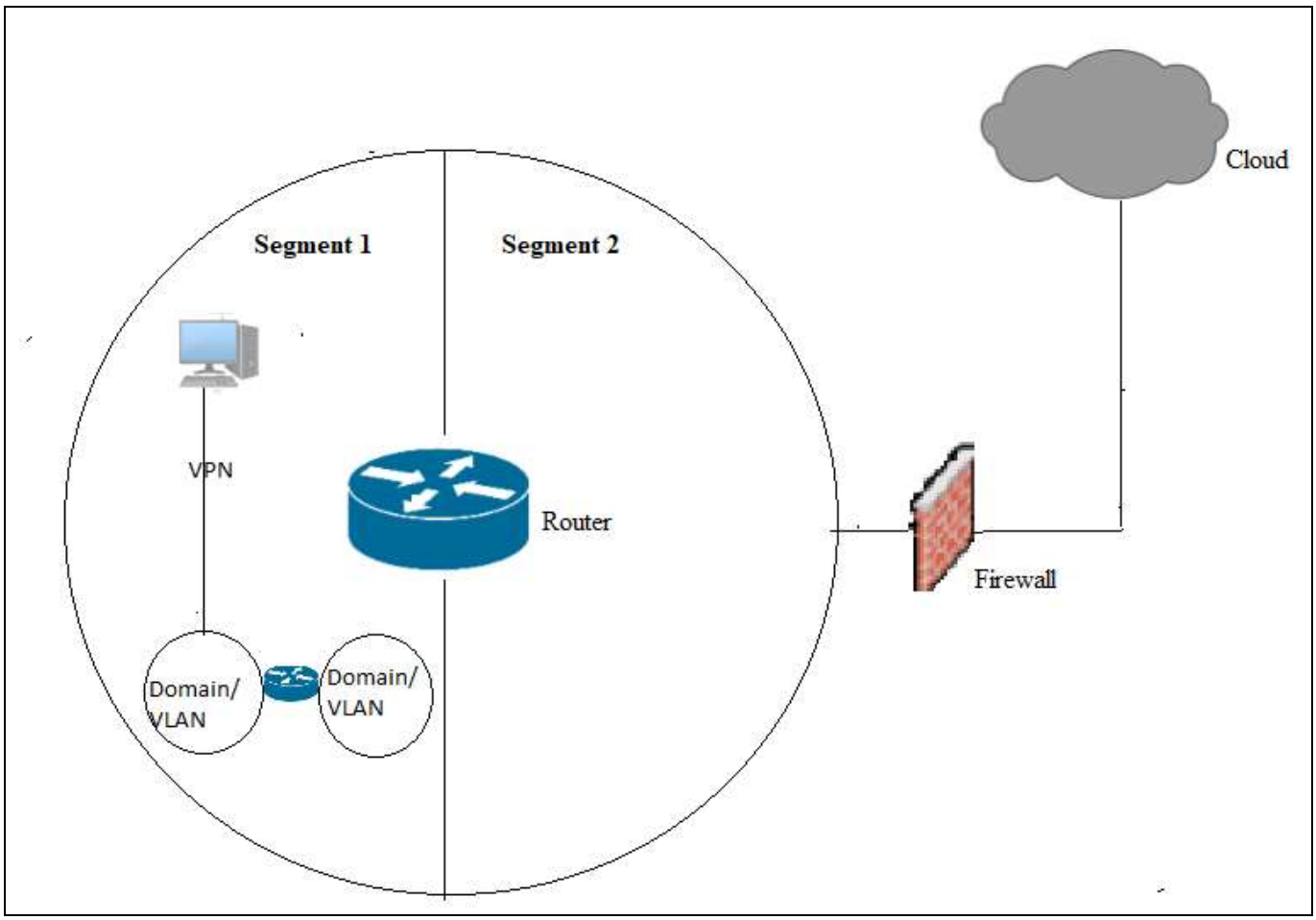

Figure 3: Proposed high-level network architecture. **Source: Author**

To implement dynamic, intelligent detection, identify the network traffic features such as protocol to submit data from client to server, source and destination IP addresses. Apply suitable feature selection techniques to select the relevant features to reduce the dimensionality and improve prediction performance.

The traffic data at the network, segment, domain, and VLAN levels are trained and assigned classes accordingly based on whether or not there is a suspected intrusion. The data is separated into training, test, and evaluation sets. Perform classification using suitable machine learning algorithms such as k-Nearest neighbours, support vector machine, and decision tree.

In the evaluation, prediction performance measures such as accuracy, sensitivity, specificity, and receiver operation characteristics are evaluated to choose the best performing algorithm. The algorithm with the corresponding script that gives the best performance should be launched as a cronjob executed at agreed intervals, and the different reports published on a dashboard to inform decision makers. Alerts at certain defined thresholds can be automatically sent to the administrator to take action if abnormal traffic in the network is detected.

4. Discussion

Cyber-attacks, targeting both private and public sectors in countries such as Uganda, are becoming bigger and more aggressive in terms of effect and cost (NRD, 2019). Cyber-attack may infringe on individual privacy, lead to access to personal data, or bring

down a network. This results in a lack of customer trust and loss of revenue for telecommunication operators with reputational damage. Companies, however, may not easily share the accurate value of losses from cyber-attacks for fear of this damage. Cyber-attack threat has been described by countries such as the United States of America as one of the gravest national security dangers (White House, 2015).

Uganda enacted a law on data protection and privacy in 2019 (Republic of Uganda, 2019) with the National Information Technology Authority –Uganda (NITA-U) as a regulator to monitor any oversight roles by data collectors and processors. National Information Technology Authority, as a regulator, has put in place necessary processes, policies, standards, and guidelines to help in information assurance. The NITA-U has availed a National Information Security Policy, which is a minimum security control for all public and private sector organisations. This is within the National Information Security Framework on security standards and technical risk assessment. However, the mandated minimum requirements contained in this policy define baseline security controls only, and organisations have to do more than merely apply the basic security controls. It's further advised by NITA-U that organizations must determine the additional security controls that they must apply to mitigate, to acceptable levels, the cyber threats relevant to their business activities (National Information Technology Authority - Uganda, 2014). On this basis, this work makes further suggestions on how to safeguard critical infrastructure in ways such as paying attention to common attack vectors and payloads, identification of attack gates, critical infrastructure, and mitigation against attacks on such infrastructure. In comparison to other areas, the European Union (Politou *et al.*, 2018) has put in regulations guarded under the General Data Protection Regulation's (GDPR) application to enforce new legal requirements for the protection of personal data and privacy of individuals to be enforced by data controllers operating within the European Union territory. This underscores the importance of data protection from attackers in both the private and public sectors.

Telecommunication companies in Uganda have the ardent task of guarding against their data and critical infrastructure to avoid unauthorized access to confidential information and network downtime. This requires safeguarding against the attack vectors, constant monitoring of the attack gates, and the critical infrastructure. As argued by Romanosky (2016), firms have an incentive to identify attacks against their corporate systems and networks to avert attacks and reduce losses. This study identified the attack vectors as Viruses, e-mail attachments, web pages, User API, Pop-ups, Social engineering, Phishing, and Malware. The attack gates identified were usernames and passwords, disgruntled employees, poor data encryption standards, misconfiguration in the cloud, servers, routers and switches, cookies, third-party vendors/platforms (3PP), user APIs, and web browsers, amongst others. Robust security checks and monitors should be put in place to validate details such as permissions, profiles, details in cookies, and exploitable vulnerabilities from both the API providers and developers before accessing any data or information.

The critical infrastructure needs close monitoring to ensure no entry or access through them to avoid attacks against the corporate systems and networks. The mitigation measures to avoid access suggested in this study include, amongst others, strict IT policy guidelines, regular deployment of patches frequently, formulation of a change advisory board (CAB) committee to analyze and approve any change in the systems, frequent system auditing, separation of testing and production environment. The government is expected to take a keen interest in safeguarding the equipment as well since telecommunication companies contribute enormously to the national revenue. As reported by the Ministry of Finance (2019), the number of mobile phone subscriptions in the country rose from 19.5 million in 2014 to 24.8 million in 2018. The national tele-density increased from 53.3 percent in 2014 to 61.1 percent in 2017, while internet subscriptions increased from 4.1 million in 2014 to 18.1 million users in September 2017 (Ministry of Finance, 2019). The telecommunications sector in Uganda has, therefore, become a major source of tax revenue for the government treasury.

In the wake of situations such as the coronavirus (COVID-19) outbreak, which is a global pandemic, most companies have encouraged employees to work remotely from home to avoid concentration so as to reduce and slow the transmission of the virus. Cloud computing and smart technology are being utilized to access company resources. This type of work schedule relies on having internet connectivity with technologies such as a virtual private network (VPN) or remote desktop setup to securely connect to applications and data hosted on the internal company network, notwithstanding good data transmission speed. Cyber attackers can target this kind of connectivity to access company data if not properly secured. To minimize the attack through poorly constructed APIs, which become weak entry points, aggressive penetration testing, which checks for exploitable vulnerabilities both from the API provider and developer points, is being carried out frequently by telecommunication companies.

During the same COVID-19 pandemic, the mobile money platform has become a critical telecommunications infrastructure and a critical national infrastructure in Africa. It is the most recommended tool for financial transactions in an attempt to avoid transmission of the disease from infected persons through the direct physical exchange of money as a medium of financial transaction.

The bubble security framework can be built on the backbone of the work of researchers such as Idhammed *et al.* (2018), who suggested a technique to insert the detection system in the Cloud side by side with the edge network components of the Cloud provider. This facilitates the interception of incoming network traffic to the edge network routers of the physical layer. Other researchers, such as Sung *et al.* (2011), suggested a detection technique that utilizes intelligent mobile agents that are distributed throughout the enterprise network to collectively monitor user activities, build user profiles, evaluate intrusion risk, match user activities with known attack patterns and signatures, and perform intrusion determination. Such a framework, when adopted, would continually sound an accurate alarm in case of an attack and enable real-time intervention to avoid loss due to exploits by attackers. This study supports the argument by Jang-Jaccard and Nepal (2014) that cyber-attacks and defense strategies should enforce the preservation of confidentiality, integrity, and availability (CIA) of any digital and information technologies. The implementation and evaluation strategy suggested will strengthen the monitoring and control of network infrastructure devices such as routers and firewalls. Ganapathy *et al.* (2012) implemented an intelligent agent-based enhanced support vector machine algorithm for mobile ad.hoc networks. Some techniques used for feature selection could be adopted from this work.

5. Conclusions and Recommendations

5.1 Conclusions

The study identified the common motivations of cyber-attacks and the attack vectors used. The attack gates and corresponding defense mechanisms to minimize vulnerability have been suggested. The critical infrastructure vulnerable to cyber-attacks has been identified, and mitigation measures to curtail attacks have been proposed. The study suggests a framework to enhance timely intrusion detection of cyber-attacks. This could go a long way to improving the safeguarding of the company's confidential information and critical infrastructure.

However, due to the change in the technological landscape influenced by rapid growth and advancement, there could be other plausible remedies that are not mentioned in this study. This is motivated by advancements and innovations of cutting-edge technologies to avert cybercrime and protect critical infrastructure.

5.2 Recommendations

We recommend that telecommunication companies enforce end-user training to create awareness among employees as a primary intervention measure.

Companies should build profiles on users, accounts, clients, contractors, and others associated with the business, which can be used for future transaction authentication.

Continuous monitoring of the critical infrastructure and attack gates should be made part of the overall risk management process of a telecommunication company, and innovations in cybersecurity detection and prevention should be harnessed.

The IT policy should include the segregation of roles, an incidence response plan, the frequency of cyber risk assessment, and security protocols and procedures.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Bank of Uganda (2019). Financial Stability Report, *Report*, Issue 11, 1-42.

[2] Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory. *MIS Quarterly*, *1*(4), pp. 11-28.

[3] Buttell, A. E. (2010). 6 Reason to Switch to Cloud Computing, *Journal of* Financial *Planning*, Practice Management, pp 6-7.

[4] Conboy K., Fitzgerald G., and Mathiassen L. (2012). Qualitative methods research in information systems: motivations, themes, and contributions, *European Journal of Information Systems*, *21* (2), pp 113-118.

[5] Corbin J. M. and Strauss A. L. (2008). Basics of qualitative research: techniques and procedures for developing grounded theory. 3rd ed. Thousand Oaks, CA: SAGE.

[6] Ganapathy S., Yogesh P. and Kannan A. (2012). Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM. *Computational Intelligence and Neuroscience*.

[7] Garisson, G., Wakefield, R. L. and Kim, S., 2012. Success Factors for Deploying Cloud Computing, *Communications of the ACM*, 55 (9), pp 62-68.

[8] GSMA (2019). Mobile Telecommunications Security Threat Landscape.

[9] Idhammad, M., Afdel, K., and Belouch, M. (2018). Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques, *Procedia Computer Science*, Volume 127, pp 35-41.
[10] Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, *80* (5), pp 973-993.
[11] Keijo H and Pekka T., (2008). Practical Man-In-The-Middle Attacks Against Bluetooth Secure Simple Pairing, In *Proceedings Wireless Communications, Networking and Mobile Computing*, pp. 1-5.
[12] Lee K., Kim J., Kwon K.H., Han Y. and Kim S. (2008). DDoS attack detection method using cluster analysis. *Expert Systems with Applications*, *34* (3), pp 1659-1665.
[13] Ministry of Communication and Information Technology, India (2012). Security Testing in Telecom Network, *White Paper*.
[14] Ministry of Finance, Planning and Economic Development (2019). Background to the budget fiscal year 2019/20, *Report,* pp 1-264.
[15] National Information Technology Authority – Uganda (2014). National Information Security Framework Publication.
[16] NRD (2019). Cyber Defense East Africa, NRD *Cybersecurity*, Vilnius, Lithuania.
[17] Politou, E., Alepis, E. and Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4 (1), 1-20.
[18] Ramadani, S., Siahaan, A. P. U., Sutrisno, Ritonga, S., Amelia, W. R., Dalimunthe, H. and Munthe, R. (2018). Impact of Cybercrime on Technological and Financial Developments, *International Journal for innovative research in multidisplinery field*, *4* (10), pp 341 – 344.
[19] Romanosky, S., (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2* (2), pp 121–135.
[20] Siponen, M.T., and Oinas-Kukkonen, H. (2007). "*A Review of Information Security Issues and Respective Research Contributions*," ACM Sigmis Database, *38* (1), pp 60-80.
[21] Smith, R.G. (2007). Crime Control in the Digital Age: An exploration of Human Rights Implications, *International Journal of Cyber Criminology*, *1* (2), pp 167–179.
[22] Sung, A. H., Mukkamala, S. and Lassez, J. (2011). Computationally intelligent agents for distributed intrusion detection system and method of practicing same, United States Patent 7941855.
[23] The Republic of Uganda (2019). Data Protection and Privacy ACT, Kampala, Uganda.
[24] Uganda Communication Commission, (2019). Telecommunications, Broadcasting & Postal markets Industry Report Q3, *Report*, pp 1-18.
[25] Venkatachary, S. K., Prasad, J. and Samikannu, R. (2018). Cybersecurity and cyber terrorism - in energy sector – a review, *Journal of Cyber Security Technology*, *2* (3-4), pp 111-130.
[26] White House (2015). Cyber Threat Intelligence Integration Center. The White House, Office of the Press Secretary.
[27] World Economic Forum (2018). The Global Risk Report, *Report*.
[28] Yin R. K. (2014). Case Study Research Design and Methods (5th ed.). Thousand Oaks, CA: Sage. 282 pages. *The Canadian Journal of Program Evaluation*. *30* (1). *DOI: 10.3138/CJPE.BR-24*.
[29] Zaini M. K., Masrek M. N., Sani M. K. J. A., and Anwar N. (2018). Theoretical Modeling of Information Security – Organizational Agility Model based on Integrated System Theory and Resource Based View. *International Journal of Academic Research in Progressive Education and Development*, *7* (3), 390–400.