ISSN No:-2456-2165

Network Security Algorithm for Forensic Management in Uganda Government Agencies

Ssonko Denison, Francis Lowu, Adam Alli. A
Department of Science and Technology
School of Gradaute Studies, Bugema University
P.o Box 6529 Kampala

Abstract:- This research focuses on proposing a network security algorithm for forensic management in Uganda government agencies. With the increasing dependence on technology, the risk of cyber-attacks and data breaches has become a major concern for government agencies, making it essential to develop effective security measures. The network security algorithm is based on machine learning, a method of data analysis that automates analytical model building to detect and prevent cyber-attacks, as well as to provide efficient forensic analysis of any security incidents that may occur. The algorithm was validated for accuracy, true positivity rate of traffic, and knowledge to capture network intruders. This was achieved using Python's pycharm IDE environment and Google Collaborator to show how the normal and attacked traffic flow. A mixed-methods approach was used, including a survey of government agencies and interviews with cyber security experts in some agencies to gather information on the current security measures and identify areas that need improvement. The algorithm integrates various security technologies such as intrusion detection systems, and data encryption to provide a multi-layered defense system.

Keywords: - *Network Security, Algorithm, Forensics, PyCharm, DDOS, Government Agency*

I. INTRODUCTION

As the world is rapidly being transformed by digital technologies towards cloud computing, there is an alarming rise in cyber-attacks hence requiring the development of effective security solutions for the cloud environment, internet is playing a progressively vital role as an information infrastructure across the world, which is enabling both the e-pay and e-business sectors to boom due to its benefits and convenience for users (Tyler, 2020). However, there are numerous security threats that are still posing a big challenge to internet security. Research shows that abuses like internet worms, phishing attacks, SQL Injection Attacks, Drive-by attacks, Birthday attacks, and spam, as well as e-crime attacks, are increasingly initiated by various attackers. In order to protect different end systems from attacks, there is a need to deploy edge network anti-virus gateways, intrusion detection systems, and firewalls (Du, Le-Khac & Scanlon, 2017). According to Srinivasan & Ferrese, (2019), much as some malicious attacks that have fixed patterns can be matched to known threats, others such as Distributed Denial of Service (DDoS) attacks are sophisticated, evolve quickly, have fewer characteristics, and can be distributed over the internet. With the rapid growth of cloud adoption in both private and public sectors globally, the cloud computing environment has become one of the prospective battlefields for cyber attackers where one of the major challenges of cloud computing is the protection of data from various attacks (Du, Le-Khac & Scanlon, 2017). Mostly, Cloud services are provided by the service providers where data security is a major concern for the client (Brady, 2018). The call for more solutions for such threats is proposed along with exposure to various issues related to data security in the cloud and the various challenges faced by forensic experts in the cloud. A model based on a trusted third party (TTP) along with a cloud forensics investigation team (CFIT) proves to be a better solution to enhance the trustworthiness of the service provider and thereby facilitate the cloud providers to trap cyber attackers with a strong collection of evidence which might help in the further legal process (Srinivasan & Ferrese, 2019).

Cloud computing has transformed the IT industry, as services can now be deployed in a fraction of the time that it used to take. Scalable computing solutions have spawned large cloud computing companies such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure (Brady, 2018). With a click of a button, personnel can create or resettle entire infrastructure for a computing resource in three different cloud computing service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Årnes, 2017). Forensic issues that are unique to cloud computing are controlled and dependent on cloud service providers (CSPs). Cloud forensics is a subset of digital forensics based on the unique approach to investigating cloud environments. CSPs have servers around the world to host customer data. When a cyber-incident happens, legal jurisdiction and the laws that govern the region present unique challenges (Srinivasan & Ferrese, 2019). A court order issued in a jurisdiction where a data center resides was not applicable to the jurisdiction of a different host in another country. In modern CSP environments, the customer can choose the region in which the data reside, and this should be chosen carefully.

The main effort for an investigator was to ensure that the digital evidence has not been tampered with by third parties so it can be admissible in a court of law (Årnes, 2017). In PaaS and SaaS service models, customers must depend on the cloud service providers for access to the logs as they do not have control over the hardware (Brady, 2018). In some cases, CSPs could sometimes intentionally hide the details of the logs from customers. In other cases, CSPs have policies that do not offer services to collect logs (Srinivasan & Ferrese, 2019). Du, Le-Khac, and Scanlon (2017) asserted that the practice of cloud computing forensics needs a blend of various digital forensic skills depending on the category of cloud under investigation. Although governments have frequently tried hard to create several frameworks pitched toward public services, Shumba (2018) asserted that the frameworks have not often been successful due to the available information security risks. Several governments in Sub-Saharan Africa are deploying cloud systems to mainly address well-organized provisioning of commodity Information Technology (IT) services and data center consolidation (Brady, 2018). However, as better public services strengthen, government agencies become more and more interdependent (Årnes, 2017).

This study identified these risks that are associated with information security, most especially on how cloud deployment can greatly support various services that are directly provided across different government agencies or to the public. A number of government agencies are continuing to develop new systems for cloud-based services (Vinh-Doyle, 2017). However, they need to be informed of the high risks involved so that they do not get exposed to different financial, legal compliance, technical, and information security risks. From a legal perspective, Chen (2014) noted that there is a need for legal redefinition when dealing with cloud systems in order to apply responsibilities and legal roles to each of the key parties and to properly define legal evidence standards when recovering evidence from a cloud environment. In addition, Chen refers to the requirement for clarification on the expectation of privacy laws for data that is hosted with a third party. This would only apply to the public, hybrid, and community Cloud deployment however as the private deployment is still within the perimeter of the organization.

The Manifesto is supported by over 50 members of civil society, industry organizations (such as the Center for Democracy and Technology, World Wide Web Foundation, Cyber Threat Alliance, and Derechos Digitalis), and individuals. Signatories to the Manifesto want to also ensure that any cybercrime convention preserves and upholds basic human rights and freedoms guaranteed under existing international UN and other treaties (CIPESA, 2021). According to (Africa Cyber Security Report – Uganda, 2019/2020), the decision in Stella Nyanzi vs. Uganda Criminal Appeal 0079 of 2019 introduced questions of digital identity and evidence in the process of judicial consideration. From this decision, it is apparent justice system has to go in appreciate the intersection between the judicial process and computer-related legislation. The cases of Amongin Jane Francis v. Lucy Akello HCT 01 CV EP 0001 of 2014 and Nakato Mary Annet v. Babirye Veronica Kadogo EP 18 of 2016 both of which dealt with questions of admissibility of digital evidence show that the courts in Uganda are only starting to define the key terms on what amounts to digital evidence. All these court decisions reflect an abiding challenge with regard to technical capacity among stakeholders, and with defining scope and implementation.

The Data Protection and Privacy Act (DPPA) approved by the President of Uganda On the 25th of February 2019, was set up to protect the privacy of individual and personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected (Ugandan citizens) and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and is inspired by the GDPR of the European Union. (“THE DATA PROTECTION AND PRIVACY BILL”, 2019). In Uganda, government ministries, departments, and agencies have already made moves into cloud computing (NITA, 2018). For example, in the National Information Technology Authority – Uganda (NITA - U), Uganda Revenue Authority (URA), Uganda Registration Services Bureau (URSB), and Kampala Capital City Authority (KCCA), over 300 public civil servants or government employees already have unlimited access to various services such as Gmail and Google documents (NITA, 2018). The URA has moved its government-wide portal to the cloud, especially during this period when everyone is required to keep at least 4 meters of social distancing due to the COVID-19 pandemic. Hence tax-payers are remotely paying their taxes.

In Uganda, an increase in remote connections by over 30% prompted an increase in working from home due to the Covid-19 pandemic, which caused several cyber-attacks in the year 2020 (The Africa Cyber Security Report, 2020). For example, in March 2020, which was the period of the lockdown, vulnerabilities rose to 1,640, representing a 21% increase (The Africa Cyber Immersion Centre Researchers, 2020). On the same note, among the most serious attacks in Uganda was the mobile money heist, in which it was alleged that banks and telecom companies including Bank of Africa, Stanbic, Airtel, and MTN were robbed of Shs7b (The Africa Cyber Immersion Centre Researchers, 2020). Investigations pointed out that some staff the aggregator, Pegasus Technologies assisted some network of suspects (Kasemiire, 2021).

According to National Information Technology Authority – Uganda, the authority issued a Public Key Infrastructure (PKI) License to Pos Digicert. PoS Digicert, Mantra Technologies, and Digital Trust are part of the Joint Venture that was contracted by the Government of Uganda to establish and maintain the Digital Authentication and Electronic Signatures solution under the brand name UGPASS, which supports the use of advanced electronic signatures based on trusted and secure Public Key Infrastructure. This brings forth for the first time advanced electronic signatures compliant with the Electronic Signatures Act and as such admissible in Courts of Law. (NITA-U Press release, 26. April 2022).

II. PROBLEM AND MOTIVATION

There is a growing rate of cyber-attacks in Uganda which is mostly due to an increase in remote connections by over 30% since the year 2020 (The Africa Cyber Security Report, 2020) and an increase in the use of cloud services (CIPESA, 2018). The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (2018) indicates that information security in Uganda has increased in importance to help protect government Ministries, Departments, and Agencies (MDAs) networks from risks of cyberattacks and security breaches. Over 77.3% of the MDAs in Uganda have developed an information security policy, but it is unclear how many of them have fully implemented their security policies and monitored compliance on a regular basis (CIPESA, 2018). As MDAs increasingly use digital technologies, digital forensics, and information security become more crucial to help protect their networks from information security risks such as cyber-attacks (CIPESA, 2018). Several cloud services are greatly growing in Uganda's MDAs but information security risks and the digital forensic algorithms for investigating them have not been well envisioned (CIPESA, 2018). Government agencies and businesses created end-to-end digital channels by providing digital certificates for natural persons and qualified electronic seals for legal entities, electronic signatures used under public key encryption which can be forged and intruders get unauthorized access to both the digital signatures and network resources of which this problem was not given a mechanism of capturing the attackers or intruders. There is still a gap to detect and capture the criminals behind the network attacks. This problem of attacks needs a hybrid machine learning technique security algorithm of data mining using KDD and intrusion detection to capture the criminals behind these attacks. In this study, a Network security algorithm for forensic management to establish a secure IT infrastructure environment was designed with the help of a team that consists of cloud customers, cloud providers, Trusted Third parties, and Forensic investigators.

III. OBJECTIVES

The objectives of this study were as follows:

- To explore existing network security algorithms for forensic management of digital files for requirements elicitation.
- To design and develop a network security algorithm for forensic management.
- To experiment with the performance of the algorithm.

IV. RELATD WORK

The cloud architecture mainly provides three categories of services IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) (Montasari, 2018). The four well-known deployment models used in cloud computing are Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud (Montasari, 2018). In a traditional forensics' environment, the internal security team has control over who is conducting forensics operations on a machine, whereas in cloud forensics, the security team has no control over whom the CSP chooses to gather evidence. If they are not trained according to a forensic standard, the chain of custody may not hold in a court of law (Montasari, 2018). Digital forensics is the application of informatics to assure proper presentation of computer crime evidentiary data into a court by mainly preserving the integrity of them and maintaining a strict chain of custody". The ultimate goal of digital forensics is to obtain evidence so that the 5Ws and how (5WH) questions can be answered (WILEY, 2017). The 5WH questions include what happened, who was involved, when did it take place, where did it take place, why did that happen, and How an incident occurred. Answering these questions leads to confirming or refuting allegations of an incident.

The word Forensic refers to all the science and technology used in the solving of crime. The aim of this Forensic Management System is to manage the large volumes of data that are produced in the process of solving crimes by the application of scientific methods and modern technology. A cyber-criminal can be described as a person who legitimately involves in the destruction of privacy or security of data and utilizing unauthorized resources causing loss to the digital users (Zawoad & Ragib, 2013). The cloud computing environment is becoming a battlefieldield of cybercrime where new challenges are being posed to defend the cyber-attacks. To meet the challenges of digital data threat, a network security algorithm for forensic management and digital forensics models was applied over the remote servers of the cloud, giving way to a new term called cloud forensics.

Montasari (2018) defined cloud computing as both the applications delivered as different services online and systems software or hardware in the data centers that deliver those services. Caviglione, Wendzel & Mazurczyk (2017) outlined 4 cloud delivery models, public, private, hybrid, and community clouds, among which government agencies, departments, or ministries may employ a model or a group of distinct models for the optimized or efficient provision of business services and applications. In the public cloud, all cloud services can be accessed by the public and can be owned by an agency or organization selling them. In a private cloud, all cloud services can solely be accessed by an organization or agency and can be managed by a third party or the organization. In a hybrid cloud, there are various cloud computing infrastructures, which include private, public, or community. While in a community cloud, Caviglione, Wendzel & Mazurczyk (2017) noted that cloud services can be managed by a third party or organizations and often shared by various agencies for supporting a given community that has shared concerns such as security requirements, mission, and policies.

- *Algorithm*

It refers to a sequence of finite steps and procedures used to solve a particular problem.

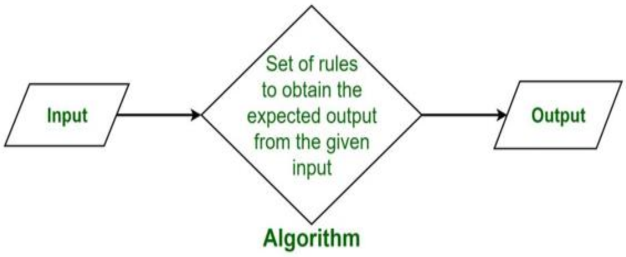

Input
Set of rules to obtain the expected output from the given input
Output
Algorithm

Fig 1 Algorithm

- *Existing Network Security Algorithms*

Existing security algorithms used by the government agencies in the I.T infrastructure include;

RSA is a Public Key algorithm that provides security by encrypting and decrypting the data so that only authorized users can access it. RSA stands for Ron Rivest, Adi Shamir, and Len Adleman, who first described it in 1977. The data is encrypted, and the ciphertext is then stored in the cloud. When a user needs the data, the user places a request to the cloud provider, then authorizes the user and provides him with the data.

The digital signature algorithm (DSA) refers to a digital signature standard. The National Institute of Standards and Technology (NIST) introduced it in 1991 as a better method for creating digital signatures. Along with RSA, DSA is considered one of today's most preferred algorithms for digital signatures. DSA does not encrypt message digests using a private key or decrypt message digests using the public key. Rather, it uses unique mathematical functions to create a digital signature consisting of two 160-bit numbers originating from digests of the message and the private key. DSAs use the public key to authenticate the signature, but when compared with RSA, the authentication process is more complicated. Message-Digest Algorithm 5 (MD5) is a cryptographic hash algorithm that can be used from an arbitrary length string to create a 128-bit string value. Though insecurities with MD5 have been identified, it is still widely used. MD5 is most commonly used for checking file integrity. It's also used in other security protocols and applications like SSH, SSL, and IPSec, however. Some applications reinforce the MD5 algorithm by adding a salt value to the plaintext, or by applying multiple hash functions.

V. METHODOLOGY

The researcher used the qualitative method for exploratory purposes and practical analysis. Using the qualitative method, the researcher got in-depth knowledge of different cloud service providers and cloud services with respect to information security and the risks involved. While with the qualitative method, the research achieved the first specific objective of exploring existing network security algorithms for the forensic management of digital files through a literature review.

The study took a design science approach method to enable analyzing and understanding suitably the problem. To conduct research and answer the questions the researcher also used two of the largest and most well-known data sets currently available to the public. The two data sets of knowledge discovery data set and the IDS data set. The two data sets aimed at providing low-level data of network traffic communication by including traffic that is considered as normal (non-malicious) and malicious.

Table 1: Comparison of IDS Datasets

Dataset	Year of Inception	No Observations	No of Fields	Classes
CIC IDS	2019	225,745	79	Benign DDoS
NSL-KDD	2021	125,973	42	Anomaly Normal
*Only data from the Friday file.				

The IDS dataset provides data in a comma-separated format (CSV), while the knowledge discovery in databases dataset provides *arff* files that are native to the WEKA package, which formats can be read by almost all programming languages which allowed the researcher to run virtually any classifier wanted.

The two specific datasets were chosen for multiple reasons:

- The significant age difference between the two (2019 – 2021) might indicate that the latter was able to identify newer threats.
- Significantly different observation and field sizes. This might help answer the question of whether a larger dataset is better for Intrusion Detection.

- *Lack of research based on the IDS dataset.*

The tools that attackers had were advancing exponentially, with more and more ways of intrusion being discovered. Due to that, the field of Cyber-Security needs to perform frequent testing and help the datasets grow so that they can detect and deter more "modern" attacks.

Intrusion Detection is a time-sensitive task that if not handled on time, could have devastating results. In the end, having an algorithmic model that could run inference on incomingdata inreal or close to real-time, is essential to deter said attacks. While this paper did not directly compare the inference time between the algorithms, it was still an incredibly significant part of the entire Intrusion Detection effort. To compare the performance of the datasets, they were run through several different classification algorithms. All models use the same settings across both datasets to ensure a clear view of how the actual dataset affects performance. Saranya et al. (2020) found that the Random Forest classifier has outperformed all other tested classifiers by a significant margin with an Accuracy rate of 99.65%. There is, however, no shortage of classifiers that can be a great fit for an Intrusion Detection system and this paper aimed to run most of the major classifiers on the two datasets mentioned above.

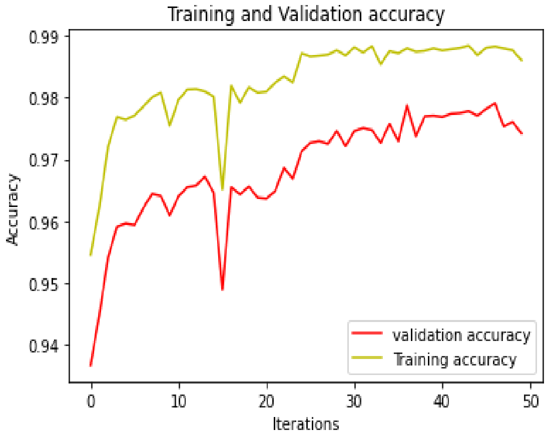


Fig 2: Training and Validation Accuracy

The Random Forest deployed several different decision trees and applied them to sub-sections of a given dataset. The Random Forest classifier then combined the outcome of the decision trees to significantly increase the prediction accuracy

VI. STUDY POPULATION

The population targeted has a group of members that a researcher was most interested in for the study (Shahrokh & Dougherty, 2014). The target population of the study was the employees in the government cloud service-providing departments, agencies, or authorities including; the National Information Technology Authority – Uganda (NITA - U) and URA.

VII. VALIDITY & RELIABILITY

In order to make sure that quality and relevant data was collected, the research instruments were tested for validity and reliability as follows: To establish validity qualitatively, the questionnaire was given to an expert (I.T supervisor) to evaluate the relevance of each question in the instrument item to the objectives and rate some of the questions on the scale of Strongly Disagree (1), Disagree (2), Not Sure (3), Agree (4) and Strongly Agree (5). Validity in research measurement refers to the extent to which the test measured what it claimed to. For reliability, the extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability to factors such as researcher bias, errors in measurement, and inconsistency of the procedures used". Interpretivist however suggested that the research is reliable as long as the researcher can demonstrate interpretive algorithm accuracy.

VIII. RESULTS & ANALYSIS

To analyze the algorithm, two of the currently most popular datasets available for Intrusion Detection were used. The two datasets are the IDS and Knowledge Discovery in Database. The two datasets differ in various ways which could lead to one of the two to stand out in terms of their predictive capabilities. IDS datasets use the notion of profiles to generate datasets in a systematic manner, which will contain detailed descriptions of intrusions and abstract distribution models for applications, protocols, or lower-level network entities, and KDD datasets are an iterative process where evaluation measures can be enhanced, mining can be refined, new data can be integrated and transformed in order to get different and more appropriate results.

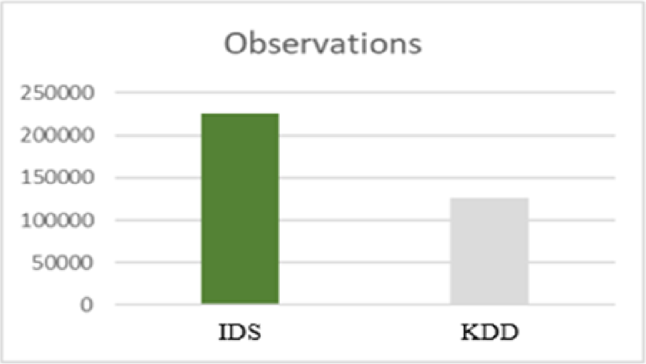


Fig 3: Observations of Datasets

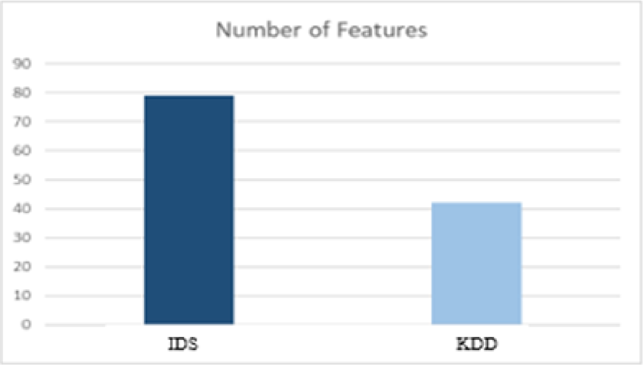


Fig 4: Number of Features

Understanding the difference between the two is essential to gain a greater insight as to what constitutes a concrete Intrusion Detection dataset.

The IDS dataset is a collection of data points from simulated attacks on a controlled network. It provides network features extracted from normal/benign traffic but also from various different attack types such as DDoS ("Distributed Denial of Service"), Port Scan, Infiltration, and more. For this research, the different kinds of attacks were merged under the "anomaly" class to create a composite binary class and provide a dataset that more closely resembles NSL-KDD. This research did not assess the capability of a model in cherry-picking out the difference between various attacks.The dataset provides two sets of data, the original PCAP files with the network trafficlog and CSV files which are derived from running the PCAP files through CICFlowMeter, a feature extraction tool that extracts network features from PCAP files in plain text. The resultant 78 network features consist of various metrics of network traffic such as the duration of the flow of data, the port number that the communication was forwarded to, various metrics on the packet size, and much more.

Table 2. IDS Class Distribution

Class	Frequency	Percentage
Benign	97718	43.28%
Malicious	128027	56.71%

Intrusion Detection is well known to be a very imbalanced problem, meaning that theoccurrence of malicious network traffic happens at a significantly lower rate than normal traffic. While normal traffic is logged all the time, malicious traffic can only be logged during an attack, therefore, creating a gap in the availability of malicious data points when compared to normal data points. The IDS dataset is portraying a naturally imbalanced problem as a highly balanced one. Being a research dataset, this is a requirement since an imbalanced class variable could lead to catastrophic model failures. Due to the high amount of network features available, it is important to account for dimensionality in the models.

Similarly, with the IDS dataset, the KDD provides insight into normal and anomalous traffic data. This dataset, however, provides its data mainly through *arff* files which are native to the WEKA Machine Learning package written in Java.

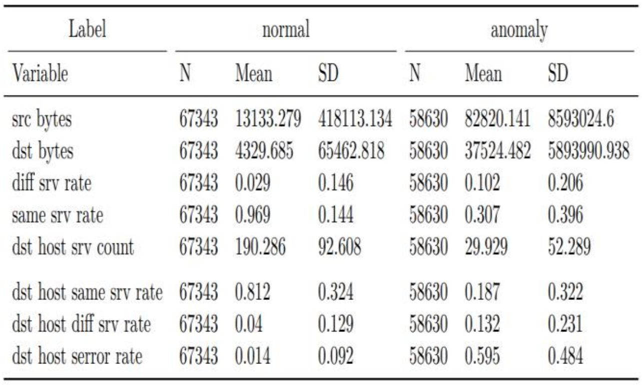
Table 3. KDD Class Distribution

Class	Frequency	Percentage
Benign	67343	53.45%
Malicious	58630	46.54%

The KDD dataset provides a significantly lower amount of data points when compared to IDS but both datasets appear to provide a balanced view to the problem in question. Both Classes (normal and malicious), appear to have an almost equal amount of data points which is very helpful in the development of an unbiased model.

The features of KDD also seem to explain the Class variable considerably well, however, when compared to IDS, the differences are significant. The top 10 selected features of the IDS explained the class variable with a weight higher than 0.5 whereas the KDD ones seem to drop below 0.5 by a significant margin. This could in theory be a major advantage of the IDS but this only became evident once both datasets have been used in Machine Learning models to detect the performance difference these could yield in a model.

Table 4. KDD Selected Features Statistics



Label	normal			anomaly		
Variable	N	Mean	SD	N	Mean	SD
src bytes	67343	13133.279	418113.134	58630	82820.141	8593024.6
dst bytes	67343	4329.685	65462.818	58630	37524.482	5893990.938
diff srv rate	67343	0.029	0.146	58630	0.102	0.206
same srv rate	67343	0.969	0.144	58630	0.307	0.396
dst host srv count	67343	190.286	92.608	58630	29.929	52.289
dst host same srv rate	67343	0.812	0.324	58630	0.187	0.322
dst host diff srv rate	67343	0.04	0.129	58630	0.132	0.231
dst host serror rate	67343	0.014	0.092	58630	0.595	0.484

With a clear understanding of how the two datasets work and what they consist of, itis important to benchmark the two against various models to understand how each classifier performs under different models. The researchers identified that the Random Forest Classifier is the best one can choose. Previous researchers however have focused on the KDD and KDD Cup 99 datasets. Running the Random Forest on a newer dataset such as the CIC-IDS, helped us identify whether the classifier was still the rightful king.

Table 5: Random Forest Performance Metric

	IDS			***KDD***	
	Benign	Malicious		Benign	Malicious
Benign	29303	0	*Benign*	67317	26
Malicious us	4	38416	*Malicious*	685	57945

Previous studies confirmed that this classifier performs exceptionally well on both our datasets. The classifier managed to achieve a 99.9% accuracy and precision scores on both datasets, providing an exceptionally low False Positive rate.

IX. ACKNOWLEDGMENT

We express our sincere appreciation to Bugema University directorate of research and publication and School of Graduate studies for their support. We also thank Uganda revenue authority (URA), department of Information technology for giving us data that helped in making an informed analysis and training of our model.

X. CONCLUSION AND FUTURE WORK

This research suggests that both freely available datasets perform quite well using certain Machine Learning algorithms. The training times are high given the amount of data; though the prediction times are relatively low which indicates that they could very well be used in a production ready model. There are although some caveats. Both datasets display a balanced approached to a wildly imbalanced problem. Both being simulated data; they assume that the distribution of normal and anomaly data points is equal which in a real-life scenario they would not be. They also offer a limited variety of class attributes such as “anomaly” and “normal” but a production-ready model should be able to identify and distinguish between different kinds of attacks and be able to “protect” the network from all of them while taking certain actions to mitigate said attacks. The older dataset, KDD, does not provide a distinction between various kinds of attacks but rather provides details as to whether a data point is normal or malicious. IDS, on the other hand, distinguishes between different attacks and it would be beneficial if future research tries to identify whether such distinction would benefit a model. It is clearly seen that the IDS dataset seems to perform better than the KDD dataset in certain situations. This could be attributed to a few key points. That is, the IDS dataset provides a significantly higherobservation number and much more features. This could mean that a researcher can select more features that explain the Class variable with a high weight. This would lead to a model that can better extrapolate the effect of a given variable on the class and easily distinguish between what is normal traffic and what is malicious traffic. The IDS dataset is also a significantly newer collection of data which is a significant advantage. As stated, intrusion attempts grow in size and sophistication every year and for that, having an updated dataset can significantly help in the effortof battling such attacks.

REFERENCES

[1.] Al Mutawa, N., Bryce, J., Franqueira, V. N., Marrington, A., & Read, J. C., (2019). Behavioral digital forensics model: Embedding behavioral evidence analysis into the investigation of digital crimes.

[2.] Albabtain, Y., & Yang, B., (2018). The process of recovering image and web page artifacts from the GPU. International Journal of Cyber-Security and Digital Forensics, 7(2), 132-142.

[3.] Alghamdi, M. I., (2020). Digital forensics in cyber security-recent trends, threats, and opportunities. Periodicals of Engineering and Natural Sciences (PEN), 8(3), 1321-1330.

[4.] Amin, M.E., (2005). Social Science Research: Conception, Methodology and Analysis. Makerere University Press, Kampala.

[5.] Association of Chief Police Officers. Practice advice on core investigative doctrine. Centrex; (2005).

[6.] Brady, O. D. (2018). Exploiting digital evidence artefacts: finding and joining digital dots (Doctoral dissertation, King's College London).

[7.] Call For Life Uganda. Retrieved 8 February 2020, from https://theacademy.co.ug/index.php/call-for-life/

[8.] Casey, E. (2019). The chequered past and risky future of digital forensics. Australian Journal of Forensic Sciences, 51(6), 649-664.

[9.] Caviglione, L., Wendzel, S., & Mazurczyk, W., (2017). The future of digital forensics: Challenges and the road ahead. IEEE Security & Privacy, 15(6), 12-17.

[10.] Choo, K. K., & Dehghantanha, A., (2017). Contemporary digital forensics investigations of cloud and mobile applications. In Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (pp. 1-6). Syngress.

[11.] Committee, 1. (2019). 100 Innovators begin pitching their innovations to the Selection Committee – Ministry of ICT & National Guidance. Retrieved 8 February 2020, from https://ict.go.ug/2019/04/16/100-innovators-begin-pitchingtheir-innovations-to-the-selection-committee/

[12.] Cyber Crime Insurance | Gold Star Insurance. Retrieved 6 February 2020, from https://www.goldstarinsurance.com/cyber-crime-insurance/

[13.] DFCU bank in crisis as over Shs10b is hacked – (Eagle Online.,2019). Retrieved 7 February 2020, from https://eagle.co.ug/2019/07/13/DFCU-bank-in-crisis-as-over-shs10b-is-hacked.html

[14.] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I., (2020). D4I-Digital forensics framework for reviewing and investigating cyber-attacks. Array, 5, 100015.

[15.] Draku, F. (2019). Hacker steals sensitive data from govt website. Retrieved 9 February 2020, f rom

[16.] Du, X., Le-Khac, N. A., & Scanlon, M., (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:1708.01730.

[17.] Forensics Science and Crime Science. Available at: http://www.staffs.ac.uk/academic_depts/sciences/subject/forensics/. (Accessed September 3, 2010)

[18.] Forensics Science Regulator – GOV.UK 2010 Available at:

[19.] Fukami, A., Ghose, S., Luo, Y., Cai, Y., & Mutlu, O., (2017). Improving the reliability of chip- off forensic analysis of NAND flash memory devices. Digital Investigation, 20, S1-S11.

[20.] Gerberding, K., & Gerberding, K., (2020). Incident Response (1/5): The 5 Benefits of an Incident Response Plan. Retrieved 7 February 2020, from https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan/

[21.] Hassan, N. F., & Jaber, H. M., (2017). Offline vs. Online Digital Forensics of Cloud-based Services. Al-Nahrain Journal of Science, 20(4), 117-124.

[22.] https://www.gov.uk/government/organisation/forensic-science-regulator (Accessed

[23.] https://www.monitor.co.ug/News/National/Hacker-steals-sensitive-data-govt-website/688334-4954262-ylmdad/index.html

[24.] Kamoga, J., (2019). Nile breweries website hacked; brewer confirms. Retrieved 6 February 2020, from https://www.theeastafrican.co.ke/news/ea/Nile-breweries-website-hacked/4552908-5363288-2tonw2z/index.html

[25.] Kasemiire, C, (2021). Risk of cyber-attacks increasing. The Monitor, Nation Media Group Uganda.

[26.] Reporter, V., (2015). AIG launches cyber insurance. Retrieved 6 February 2020, from https://www.newvision.co.ug/new_vision/news/1332440/aig-launches-cyber-insurance/

[27.] Reporter, V., (2018). Innovations to improve health outcomes unveiled. Retrieved 5 February 2020, from https://www.newvision.co.ug/new_vision/news/1475336/innovations-improve-health-outcomes-unveiled

[28.] S. Wiedmaier, P. Digital Trends and Innovations in Uganda - ICT4D Conference. Retrieved 6 February 2020, from https://www.ict4dconference.org/digital-trends-innovations-uganda/

[29.] September 9, 2010)

[30.] Ssebwami, J., (2019). Top emerging cyber-threats to worry about in 2019.