

# Cybersecurity and Cyber Forensics: Machine Learning Approach

Ibrahim Goni<sup>1</sup>, Jerome Mishion Gumpy<sup>2</sup>, Timothy Umar Maigari<sup>3</sup>, Murtala Muhammad<sup>4</sup>, Abdulrahman Saidu<sup>4</sup>

<sup>1</sup>Department of Computer Science, Adamawa State University, Mubi, Nigeria

<sup>2</sup>Department of Computer Science, Federal University, Gashua, Nigeria

<sup>3</sup>Department of Computer Science, Federal College of Education Gombe, Nigeria

<sup>4</sup>Department of Computer Science, Federal Polytechnic Bali, Taraba Nigeria

## Email address:

algonis1414@gmail.com (I. Goni)

## To cite this article:

Ibrahim Goni, Jerome Mishion Gumpy, Timothy Umar Maigari, Murtala Muhammad, Abdulrahman Saidu, Cybersecurity and Cyber Forensics: Machine Learning Approach. *Machine Learning Research*. Vol. 5, No. 4, 2020, pp. 46-50. doi: 10.11648/j.ml.20200504.11

**Received:** September 3, 2020; **Accepted:** September 22, 2020; **Published:** December 16, 2020

---

**Abstract:** The proliferation of cloud computing and internet of things has led to the connectivity of states and nations (developed and developing countries) worldwide in which global network provide platform for the connection. Digital forensics is a field of computer security that uses software applications and standard guidelines which support the extraction of evidences from any computer appliances which are perfectly enough for the court of law to use and make a judgment based on the comprehensiveness, authenticity and objectivity of the information obtained. Cybersecurity is of major concerned to the internet users worldwide due to the recent form of attacks, threat, viruses, intrusion among others going on every day among internet of things. The aim of this work is make a systematic review on the application of machine learning algorithms to cybersecurity and cyber forensics, systematic survey method was used on recent application of machine learning algorithms on cyber forensics and cyber security based on this findings it is observed that cybersecurity is based on confidentiality, integrity and validity of data, it is also noted that there are ten steps to cybersecurity; network security, user education and awareness, malware prevention, removable media control, secure configuration, managing user privileges, incident management, monitoring and home and mobile working and pave away for further research directions on the application of deep learning, computational intelligence, soft computing to cybersecurity and cyber forensics.

**Keywords:** Cybersecurity, Cyber Forensics, Cyber Space, Cyber Threat, Machine Learning and Deep Learning

---

## 1. Introduction

Cyber space has provide a dwelling environment and platform for technology today ranging from IoT, 5G, Fog, edge among others it confine to grow and expand and support all sorts of innovations in science and technology but the good and the bad [1, 3]. According to global cyber security index 2017 revealed almost half of the world population (3.5 billion users) are connected to the cyber space and they further estimated that there will be 12 billion device-to-device connections to the cyber space by 2020. It was also reported that, by the year 2020, 80% of adults on earth will have a smartphone [48], in addition to 49.7% of the total population are connected to Internet with the growth of 936%

from 2000-2017 worldwide [49]. However threat to this space is alarming day-by-day. The aim of this research work was to explore the critical research contributions in the application of machine learning algorithms in cybersecurity and cyber forensics.

## 2. Cyber Forensics

Digital forensics or computer forensics is a branch of forensic science that described the technique of forensics investigation of crimes that take place in a computer network or computer system has been used as weapon for cyber-attack or conduct a criminal activities but with the regardless of any digital device that has been used to perpetrate the crime [2].

In addition to Nickson *et al.* [3] described cyber forensics as a sub-branch of computer security that uses software and predefined techniques which is aim at extracting evidences from any form of digital device and can be presented to a court of law for criminal and/or civil proceedings provided that it satisfy this three conditions; comprehensiveness, authenticity and objectivity. Furthermore, they were able to reveal that digital forensic report should be able to show important facts about evidence; like who obtained the evidence? Where the evidence captured and was stored and what happened to the evidence. Moreover, in 2017, Rukayat *et al.*, [4] Identified the goals of digital forensics as identification of the evidence, document the crime, collection and preservation of the evidences, packaging the evidence and transporting the evidences in an untemper manner. In 2017, Anwar & Riadi [38] suggested that cyber forensics depend on the collection and analysis of incident in order to explore understand and show complex security breaches that have by-passed security mechanism. In [46] “Digital forensics can be said to be a scientific framework in system development to identify, locate, retrieve, and analyze evidence from computers, computer storage media, and other electronic devices and present the findings in a court case”. Digital forensics it was graphically represented by Mark [50] as.

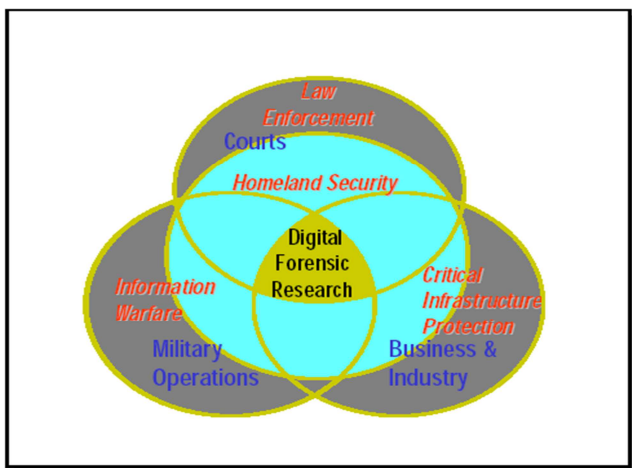


Figure 1. Digital forensics science [50].

### 2.1. Cyber Crime

Cyber threats, attacks and breaches have become a normal incident in day-to-day life of internet users [6]. Furthermore, David *et al.* [10] ascertained that cyber terrorism is a conglomeration of cyber metrics and terrorism and they also believed that cyber terrorism is an illegal use of digital devices to perpetrate damage unduly compel intimidate or further terrorist's socioeconomic political or religion agenda. Capgemini research institute reveal that in one case a hacker was able to access the GPS of 27000 vehicles which led to the shutdown the engine. “There is a pressing need for more research's and tool development to help digital investigator's obtain and analyses the increasing amount of digital evidence on smart phones, tablets, wearable devices, SatNav system,

game console, automobile, IoT systems and cloud environment [5].

### 2.2. Cyber Security

Cyber security involves data security, network security, and computer security. It is also view by many researchers as an application of security preventions to provide a sense of confidentiality, integrity and availability, of data [28] but the major objectives of cyber security are prevention detection and reaction. Moreover, CIA revealed that the main goals of cyber security are confidentiality, integrity and availability. National cyber security center UK itemize ten steps to cybersecurity; network security, user education and awareness, malware prevention, removable media control, secure configuration, managing user privileges, incident management, monitoring and home and mobile working [35]. In addition to Gyun [33] revealed that AI and machine learning are the most important cyber tools for behavioral modeling, zero-day-attacks and advanced persistent threat.

## 3. Cyber Threats

According to US intelligent community in 2016 and 2017 there has been state sponsored cyber-attack against Ukraine and Saudi Arabia which resulted in targeting major infrastructure in both government and non-governmental organizations. They further indicated that known cyber security threats are classified under the known cyber security threats are classified under three headings; identity theft which includes; phishing, spoofing, masquerading, social engineering and password crackers. Unauthorized access includes; targeted data mining, backdoor and eavesdropping and tapping. Denial of service (DoS, DDoS) includes; logic bomb and crypto-locker. Cyber security Ventures ascertained that in 2019 ransomware will damages as much as \$11.5 billion [44]. “A ransomware attack targeting England's National Health Service affected 60 health trusts, 150 countries, and more than 200,000 computer systems” [45].

## 4. Basics Concept of Machine Learning Algorithm

Machine learning is a technique of using algorithm to parse data, learn from the data and make a decision, prediction, detection, classification, pattern recognition, responding and clustering based on the data collected. These algorithms are heavenly depend on the statistical and mathematical optimization. In broader sense machine learning algorithm are used in clustering, regression, (univariate & multivariate) anomaly detection, pattern recognition [34]. The three types of machine learning are; supervised learning, unsupervised learning and reinforcement. Supervised learning algorithms are machine learning algorithms that require datasets for training and testing the performance. This dataset has to be labeled and consist of features by which events or objects are defined as well as the

expected outputs. The most common supervised learning algorithm are decision tree, logistic regression, support vector machine, relevance vector machine, random forest, K-NN, bagging neural networks, linear regression and naïve Bayes [33]. Unsupervised learning algorithm is a machine learning algorithm that required unlabeled datasets for training and testing the system performance the two major techniques used in unsupervised learning are principal component analysis (PCA) and clustering. The most common unsupervised learning algorithms are used especially in security are hierarchical, k-means, mixed model, DBSCAN, OPTIC, self-organizing mapping, Bolzan machine, auto encoder, adversarial network [34].

## 5. Literature Reviewed

In 2019, Bandir [7] he explored the used of clustering algorithms such as K-means hierarchical clustering, k-means kernel, latent dirichlet allocation and self-organizing mapping techniques for forensics analysis using text clustering in the large volume of data. In 2018, Al-Jadir et al., [8] presented a robust forensics analysis method using memetic algorithm. In 2018, Sunil & Preeti [9] revealed how artificial intelligence techniques are applied to cyber-attacks security breaches. Machine learning algorithm was used to classified malware in android system in [16]. Machine learning and deep learning algorithm are combined and used for cyber security system in [15]. Machine learning algorithms are also applied to intrusion detection system in [14, 51]. The research of [13] a systematic survey on the research that combine machine learning algorithm and data mining technique to cyber security. In 2018, Apruzzi et al., [12] presented how effectiveness of machine learning and deep learning in the feature of cyber security. Many surveys reviews and systematic reviews are conducted in the application of machine learning, deep learning and artificial intelligence techniques to cyber security, attack, intrusion detection system, network security as in some researches [16, 18-22]. Machine learning algorithm was also used to study cyber security in [29]. Security Framework was designed by [30] using fuzzy logic.

Furthermore, machine learning algorithms deep learning algorithms are applied in intrusion detection systems as in the research of A. Abubakar et al [23] presented that machine learning based system can be used to detect intrusion for software defined networks. [24] Presented an extensive survey on anomaly based intrusion detection system. [25] Applied machine learning algorithm to intrusion detection in mobile cloud in a heterogeneous clients networks. In the work of [26] hybrid intrusion detection system for cloud computing. [27] They used machine learning algorithm to provide a roadmap for industrial network anomaly detection. Anomaly detection system for automobile network was presented by [31]. Deep neural network and fuzzy logic are used to identify abnormality in network traffic [32]. A systematic survey was made by [40] on the techniques that are used for malware detection, while W. Songyang et al [41] used APIs and

machine learning algorithm to detect malware in android. In 2015, Anastasia and Gamayunov [42] presented a general review on the malware detection in mobile devices based on parallel and distributed network. [43] They made a comparative analysis between the used of static, dynamic and hybrid technique to malware detection. Forensics analysis was also made on WhatsApp messenger to identify those that are using the application to perpetrate a crime or do illegal business as in the research of [36-39]. In addition to Parag [47] Digital forensics framework was proposed and made a comparative analysis with other framework made with no AI techniques however, there framework has no instant detection and sending signals as compare to our proposed framework.

## 6. Conclusion

Machine learning algorithms are recently applied to the following area of cyber security as in network security, data security, end-point security, identity access security, cloud security, IoT security, Fog security, but majority of the security systems depend on the detection, prediction and response. Moreover, the main goals of cyber security are confidentiality, integrity and availability. In this research work it is also noted that there are ten steps to cybersecurity; network security, user education and awareness, malware prevention, removable media control, secure configuration, managing user privileges, incident management, monitoring and home and mobile working. In addition to AI and machine learning are the most important cyber tools for behavioral modeling, zero-day-attacks and advanced persistent threat.

---

## References

- [1] Shahzad S. (2015) protecting the integrity of digital evidence and basic human rights during the process of digital forensics. Ph. D. thesis Stockholm University.
- [2] Abdalzim A. M. A. & Amin B. A. M. (2015) a survey on mobile forensics for android smart phones IOSR Journal of computer engineering 17 (2) 15-19
- [3] Nickson M. K., Victor R. K. & Venter H. (2019) Divergency deep learning cognitive computing techniques into cyber forensics Elsevier Forensics Science international synergy 1 (2019) 61-67.
- [4] Rukayat A. A., Charles O. U. & Florence A. O. (2017) computer forensics guidelines: a requirement for testing cyber crime in Nigeria now?
- [5] Casey E. (2016) Editorial- A sea change in digital forensics and incident response. Digital investigation evidence Elsevier Ltd 17, A1-A2.
- [6] Ehsan S. & Giti J. (2019) Seminars in proactive artificial intelligence for cyber security consulting and research, Systematic cybernetics and informatics 17 (1) 297-305
- [7] Bandir A. (2019) Forensics analysis using text clustering in the age of large volume data: a review. International journal of advanced computer and application. 10 (6), 72-76.

- [8] Al-Jadir I., Wong K. W., Fing C. C. & Xie H. (2018) Enhancing digital forensics analysis using memetic algorithm feature selection method for document clustering 2018 IEEE international conference on systems, Man and cybernetics 3673-3678.
- [9] Sunil B. & Preeti B. (2018) Application of artificial intelligence in cyber security. International journal of engineering research in computer science and engineering 5 (4), 214-219.
- [10] David O. A., Goodness O. & Eteete M. A. (2019) Unbated cyber terrorism and human security in Nigeria. Asian social science 15 (11), 105-115.
- [11] April (2014) threat start-SMS spam volume by month of each region SC magazine. available online at <http://www.scmagazine.com/april-2014-threat-stats/slideshowz>.
- [12] Apruzzi G., Colajanni M. F., Ferreti L., & Marchetti M. (2018) on the effectiveness of machine learning for cyber security in 2018 IEEE international conference on cyber conflict 371-390.
- [13] Buckza A. L. & Guven E. (2016) A survey of data mining and machine learning methods for cyber security intrusion detection IEEE communication survey and tutorials 18 (2), 1153-1176.
- [14] Biswas S. K. (2018) intrusion detection using machine learning: A comparison study. International Journal of pure and applied mathematics 118 (19), 101-114.
- [15] Y. Xin, Kong L., Liu Z., Chen Y., Zhu H., Gao M., Hou H., & Wang C. Machine learning and deep learning methods for cyber security. IEEE Access 6: 35365-35381 (2018).
- [16] N. Milosevic, Denghantanh A., Choo K. K. R. Machine learning aided android malware classification. Computer and electrical engineering 61: 266-274 (2017).
- [17] B. Geluvaraj, Stawik P. M., Kumar T. A. the future of cyber security: the major role of Artificial intelligence, Machine learning and deep learning in cyber space. International conference on computer network and communication technologies Springer Singapore. 739-747 (2019).
- [18] H. Mohammed B., Vinaykumar R., Soman K. P. A short review on applications of deep learning for cyber security (2018).
- [19] M. Rege, Mbah R. B. K. Machine learning for cyber defense and attack. in the 7<sup>th</sup> International conference on data analysis 73-78 (2018).
- [20] D. Ding, Hang Q. L., Xing Y., Ge X., and Zhang X. M. A survey on security control and attack detection for industrial cyber physical system. Neuro-computing. 275. 1674-1683 (2018).
- [21] D. Berman S., Buczak A. L., Chavis J. S., Corbett C. L. A survey of deep learning methods for cyber security information 10 (4): (2018).
- [22] Y. Wang, Ye Z., Wan P., Zhao J. A survey of dynamic spectrum allocation based on reinforcement learning algorithms in cognitive radio network. Artificial intelligence review. 51 (3): 413-506 (2019).
- [23] A. Abubakar, Paranggono B. Machine learning based intrusion detection system for software defined networks. 7<sup>th</sup> International conference on Emerging security techniques IEEE. 138-143. (2017).
- [24] S. Jose, Malathi D., Reddy B., Jayaseeli D. A survey on anomaly based host intrusion detection system. Journal of physics. Conference series 1000 (1): (2018).
- [25] S. Dey, Ye Q., Sampalli S. A Machine learning based intrusion detection scheme for data fusion in mobile cloud involving heterogeneous clients network. Information fusion 49: 205-215 (2019).
- [26] P. Deshpande, Sharma S. C., Peddoju S. K., Junaid S. HIDS: a host based intrusion detection system for cloud computing environment. International journal of system assurance engineering and management. 9 (3): 567-576 (2018).
- [27] M. Nobakht, Sivaraman V., Boreli R. A host-Based Intrusion detection and mitigation framework for smart IoT using open flow in 11<sup>th</sup> International conference on availability reliability and security IEEE. 147-156 (2016).
- [28] A. Meshram, Christian H. Anomaly detection in industrial networks using machine learning: A road map. Machine learning for cyber physical system Springer Berlin Heidelberg. 65-72 (2017).
- [29] R. Devakunchari, Souraba, Prakhar M. A study of cyber security using machine learning techniques. International journal of innovative technology and exploring engineering. 8 (7): 183-186 (2019).
- [30] E. Alison N. FLUF: fuzzy logic utility framework to support computer network defense decision making IEEE (2016).
- [31] A. Taylor, Leblanc S., Japkowicz N. Anomaly detection in auto-mobile control network data with long short term memory network in data science and advance analytics. IEEE international conference. 130-139 (2016).
- [32] O. Amosov S., Ivan Y. S., Amosov S. G. Recognition of abnormal traffic using deep neural networks and fuzzy logic. International Multi-conference on industrial engineering and modern technologies IEEE (2019).
- [33] M. Gyun L. Artificial Intelligence for development series: Report on AI and IoT in Security Aspect. (2018).
- [34] L. Matt. Rise of machine: machine learning & its cybersecurity applications, NCC group white paper (2017).
- [35] National cyber security center UK, [www.ncsc.gov.uk](http://www.ncsc.gov.uk).
- [36] A. Nuril, Supriyanto (2019) Forensic Authentication of WhatsApp Messenger Using the Information Retrieval Approach. International Journal of Cyber Security and Digital Forensics (IJCSDF) 8 (3): 206-212 (2019).
- [37] A. Marfianto, I. Riadi. WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method. International Journal of Cyber Security and Digital Forensics (IJCSDF) 7 (3): 319-327 (2018).
- [38] N. Anwar, I. Riadi. Forensic Investigative Analysis of WhatsApp Messenger Smartphone Against WhatsApp Web-Based, Journal Information Technology Electromagnetic Computing and Information, 3 (1): 1-10 (2017).
- [39] S. Ikhsani and C. Hidayanto, WhatsApp and LINE Messenger Forensic Analysis with Strong and Valid Evidence in Indonesia. Tek. ITS, 5 (2): 728-736 (2016).

- [40] M. Ashawa, S. Morris. Analysis of Android Malware Detection Techniques: A Systematic Review. *International Journal of Cyber Security and Digital Forensics (IJCSDF)* 8 (3): 177-187 (2019).
- [41] W. Songyang, Wang, P., Zhang, Y. Effective detection of android malware based on the usage of data flow APIs and machine learning: *Information and Software Technology*, 75: 17--25 (2016).
- [42] Anastasia, S., Gamayunov, D.: Review of the mobile malware detection approaches: Parallel, Distributed and Network-Based Processing (PDP). In: *Proc. 2015. IEEE 23rd Euro micro International Conference*, pp. 600—603 (2015).
- [43] D. Anusha, Troia, F. D., Visaggio, C. A., Austin, T. H., Stamp, M.: A comparison of static, dynamic, and hybrid analysis for malware detection. *Journal of Computer Virology and Hacking Techniques*, 13 (1) 1-12 (2017).
- [44] S. Morgan, (2017). Cyber security Business Report. Retrieved from CSO: <https://www.csoononline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-b-y-2019.html>.
- [45] R. Collier, (2017). NHS ransomware attack spreads worldwide. *CMAJ*, 189 (22), 786-787. <https://doi.org/10.1503/cmaj.1095434>.
- [46] H. Trisnasenjaya, I. Riadi Forensic Analysis of Android-based Whats App Messenger Against Fraud Crime Using The National Institute of Standard and Technology Framework. *International Journal of Cyber Security and Digital Forensics (IJCSDF)* 8 (1): 89-97 (2019).
- [47] H. Parag Rughani. Artificial Intelligence Based Digital Forensics Framework. *International Journal of Advanced Research in Computer Science*. 8 (8): 10-14 (2017).
- [48] 2016: Current State of Cybercrime, RSA Whitepaper, 2016.
- [49] World Internet Users and 2017 Population Stats, accessed from <http://http://www.internetworldstats.com/stats.htm>.
- [50] R. Mark. Computer forensics: Basics. Lecture note Purdue University (2004).
- [51] Ibrahim Goni & Ahmed L. (2015) Propose Neuro-Fuzzy-Genetic Intrusion Detection System *International Journal of Computer Applications* Vol. 115 No. 8 available online at <http://www.ijcaonline.com/archives/volume115/number8/20169-2320>.