Forensic Science International: Synergy 1 (2019) 61–67

Contents lists available at ScienceDirect

Forensic Science International: Synergy

journal homepage: https://www.journals.elsevier.com/forensic-science-international-synergy/

Diverging deep learning cognitive computing techniques into cyber forensics

Nickson M. Karie [a, *], Victor R. Kebande [b, c], H.S. Venter [c]

[a] Cyber Security and Forensics Research Group, Department of Computer Science, University of Eswatini, Private Bag 4, Kwaluseni, Eswatini
[b] Internet of Things and People (IoTaP) Research Center, Department of Computer Science and Media Technology, Malmö University, Nordenskiöldsgatan, Malmö, Sweden
[c] DigiFORs Research Group, Department of Computer Science, University of Pretoria, Lynwood Road, South Africa

ARTICLE INFO

Article history:
Received 28 November 2018
Received in revised form
23 February 2019
Accepted 19 March 2019
Available online 4 April 2019

Keywords:
Cyber forensics
Deep learning
Artificial intelligence
Investigations
Cyberattacks
Cybercrimes
Framework

ABSTRACT

More than ever before, the world is nowadays experiencing increased cyber-attacks in all areas of our daily lives. This situation has made combating cybercrimes a daily struggle for both individuals and organisations. Furthermore, this struggle has been aggravated by the fact that today's cybercriminals have gone a step ahead and are able to employ complicated cyber-attack techniques. Some of those techniques are minuscule and inconspicuous in nature and often camouflage in the facade of authentic requests and commands. In order to combat this menace, especially after a security incident has happened, cyber security professionals as well as digital forensic investigators are always forced to sift through large and complex pools of data also known as Big Data in an effort to unveil Potential Digital Evidence (PDE) that can be used to support litigations. Gathered PDE can then be used to help investigators arrive at particular conclusions and/or decisions. In the case of cyber forensics, what makes the process even tough for investigators is the fact that Big Data often comes from multiple sources and has different file formats. Forensic investigators often have less time and budget to handle the increased demands when it comes to the analysis of these large amounts of complex data for forensic purposes. It is for this reason that the authors in this paper have realised that Deep Learning (DL), which is a subset of Artificial Intelligence (AI), has very distinct use-cases in the domain of cyber forensics, and even if many people might argue that it's not an unrivalled solution, it can help enhance the fight against cybercrime. This paper therefore proposes a generic framework for diverging DL cognitive computing techniques into Cyber Forensics (CF) hereafter referred to as the DLCF Framework. DL uses some machine learning techniques to solve problems through the use of neural networks that simulate human decision-making. Based on these grounds, DL holds the potential to dramatically change the domain of CF in a variety of ways as well as provide solutions to forensic investigators. Such solutions can range from, reducing bias in forensic investigations to challenging what evidence is considered admissible in a court of law or any civil hearing and many more.

1. Introduction

Technological revolutions, computer integration and the advancements in the Internet witnessed after the industrial revolution has become a staple and a sensation in all aspects of our daily lives as expressed by Refs. [1,2]. Apart from that, human beings have become dependent on Information and Communication Technology (ICT) and digital devices given that the advantages that come with these devices have helped to shape our societies. This has been realised due to the constant presence of digital information and a change that has been witnessed with the way human beings think and act [3].

Moreover, most of the computer integration techniques have seen the emergence of many computing disciplines which have brought about effectiveness. One notable area that has changed the perception of computer behaviour and how machines operate is the discipline of Deep Learning (DL) which is a subset of Artificial Intelligence (AI). DL makes it possible for multi-layered neural

* Corresponding author.
E-mail addresses: nickson.karie@gmail.com (N.M. Karie), victor.kebande@mau.se (V.R. Kebande), hsventer@cs.up.ac.za (H.S. Venter).

https://doi.org/10.1016/j.fsisyn.2019.03.006

networks to be applied in tuning machines in order to accomplish some desired tasks [4]. Actually, DL has been visualized as a state of the art approach that is able to deliver many accurate inferences, which have also changed the way intelligent decisions are made by computers [5]. Nevertheless, Cyber Forensic Science (CFS), which is a scientific process of investigating as well as excavating and proving facts in a court of law or civil hearing has seen a lot of diversifications and many techniques have been used in incident detection approaches [6,7]. As a result, this research tries to explore the dynamics of diverging DL cognitive computing techniques into Cyber Forensics (CF) in order to realise effectiveness.

In the end this research aims to device a suitable generic framework or approach through which DL cognitive computing concepts and techniques can be integrated into Cyber Forensics (CF) in order to realise effectiveness during forensic investigation using machine learning approaches. The contribution of this paper is thus, a framework for diverging deep learning cognitive computing techniques into cyber forensics.

The reminder of this paper is structured as follows: Section 2 covers the background while Section 3 handles the related work on Deep Learning and Cyber Forensics. After this, Section 4 presents an overview of the proposed DLCF Framework. Finally the paper concludes in Section 5 and make mention of the future work.

2. Background

This section presents a background study of the following areas: Cyber Crimes, Cyber Forensics and Deep Learning.

2.1. Cyber Crimes

The cyberspace is considered a domain worth exploring and investigating after land, sea and air [8]. This is mainly because of the sporadic increase in cyber-crimes and cyber-criminals [9]. The increase in cybercrimes has been necessitated by the growth in technology and the Internet. According to Ref. [10]; the globally cybercrime damages are predicted to cost $6 trillion by the year 2021. However, between 2016 and 2018 it was the most reported crime [11]. Information security timelines and statistics have shown that cybercrime is the major motivations of attacks which accounts to 81.7% as shown in Fig. 1.

Microsoft has also unearthed that, an attacker is able to reside in a network for an average of 146 days before detection [12]. This shows that cybercrime attacks are most prevalent in a network which is also a domain that forms a big part of the cyberspace. In addition, cybercrime can come in many forms or an adversary can use different techniques. Sahu et al. [13] has classified cybercrime using the following techniques: Hacking, child pornography, cyberstalking, DDoS, virus dissemination, software piracy, IRC crimes, bots, credit card fraud, phishing, etc. In the recent times, cybercrime has been regarded as an international problem which has some special challenges and can be perpetrated by state or non-state actors [14]. Research by Ref. [15], however, has shown that data mining techniques can be used to identify cyber-based attacks. For example, clustering techniques can be used in finding patterns amongst log files and/or records in the case of a forensic investigation. This therefore, has led the authors in this paper into proposing a way of diverging DL cognitive computing techniques into cyber forensics hence the birth of the proposed DLCF Framework which is discussed later in this paper. The next section briefly explains cyber forensics.

2.2. Cyber forensics

According to Ref. [7], Computer Forensics (CF) is a sub-domain or a field in computer security that makes use of software tools and some pre-defined procedures for purposes of extracting and examining a computer system. In this exercise computer-related crime evidence is extracted and then presented to a court of law for criminal or civil proceedings. In order for CF processes to be accepted, certain criteria that satisfies comprehensiveness, authenticity and objectivity of evidence has to be followed. Prior to this, CF systems could be able to allow the collection, extraction and analysis of digital evidence. A CF model presented by Ref. [16] shows how evidence can be extracted based on the following phases: Expressing Evidence, Analysing Evidence, Abstracting Evidence, Fixing Evidence and Discovering Evidence. Based on this, it is important to note that in computer forensics, data recovery is the most paramount process which in most cases can be conducted by forensic software like Encase and FTKs. A research paper by Ref. [17] also reveals that a forensic report should be able to show important facts like where the evidence captured was stored, who obtained the evidence and what happened to that evidence. These are important facts that underlie the CF techniques and processes. Because of the nature and complexity of the data that investigators have to analyse as stated earlier, errors might be introduced when this process is handled manually. For this reason bringing DL cognitive computing techniques into cyber forensics like data mining which can be used to identify cyber-based attacks and clustering which can be used in finding patterns amongst log files

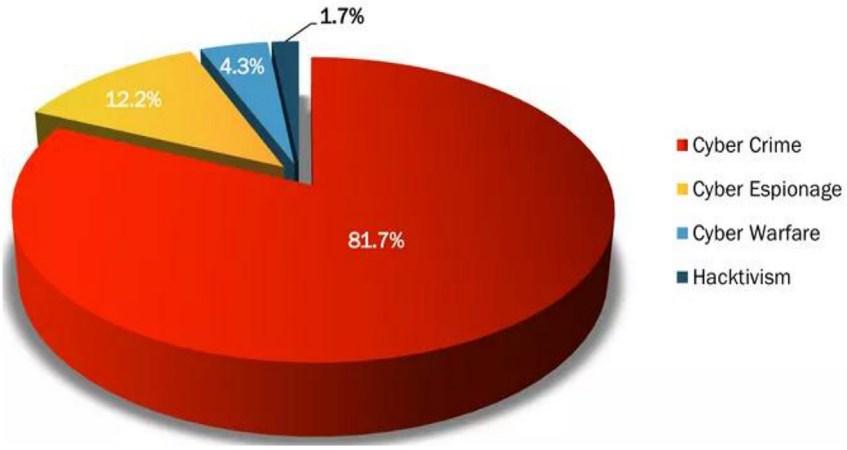

Fig. 1. Major motivation of attacks (*Source: Hackmageddon, (2018), Cyber Attacks Statistics*).

and/or records can enhance the forensic process and help in reducing bias in forensic investigations. This can further help in challenging what evidence is considered admissible in a court of law or any civil hearing. DL concepts are further explained in the next section.

2.3. Deep learning (DL)

Abbas [18] presents Deep Learning (DL) as an Artificial Intelligence (AI) function that is able to imitate the techniques of the human mind in processing. It mainly comprises of machine learning techniques that are used to represent facts. Notably Wu, Yu, Huang & Yu [19], highlights that DL is a recent development in AI that is able to be applied in multiple fields. Additionally, DL uses tools like Restricted Boltzman Machine (RBM), Auto-encoder and Convolutional Neural Network (CNN) [20] which are able to show superior performance when it comes to supervised learning tasks.

Besides being the most popular research area in machine learning, DL has come out as a scientific field that is able to offer fast processing of huge amount of data during network training. This is another reason that motivated the concept of bringing DL cognitive computing techniques into cyber forensics as a way to help in the analysis of huge amount of data during a forensic investigation process. Wang and Pei [21] also highlighted that it is possible for a Deep Neural Network (DNN) to be able to unearth visual patterns through robust learning and also huge volume of data sets. This means that DL has the ability, when used in CF, to unearth relevant PDE from Big Data as and when required by investigators. Some of the relevant related work as sampled by the authors for this paper is presented in the section to follow.

3. Related work

There exists a lot of research in Deep Learning; however, the authors acknowledge the following studies that have played a significant role in this current study.

A paper by Ref. [22] discuss the role that machine learning can play in computer forensics as well as the areas of computer forensics where machine learning techniques have been used until now. Their paper though did not specifically address the concepts of diverging DL cognitive computing techniques into cyber forensics as is the case presented in this paper. In another research, Bhatt & Rughani [23] explains how machine learning can be used in digital crime and its forensic importance, setting up an environment to train artificial neural networks and investigate as well as analyse data to find artefacts that can be helpful in any forensic investigation.

Dilek, Çakır & Aydın [24] in their paper argue that cyber infrastructures are highly vulnerable to intrusions and other threats. Physical devices and human intervention are not sufficient for monitoring and protection of these infrastructures; hence, there is a need for more sophisticated cyber defence systems that need to be flexible, adaptable and robust, and able to detect a wide variety of threats and make intelligent real-time decisions. They then present advances made in applying Artificial Intelligent (AI) techniques for combating cybercrimes, as well as detection and prevention of cyber-attacks.

Finally Mitchell [25] in his article, talks about how useful AI might be when used in digital forensics and this gave the authors a motivation and a research focus worth exploring with the main aim of proposing a framework for use in cyber forensic investigations. While the above mentioned research studies remains useful and insightful, none of these studies was focused on a framework specifically meant for diverging DL cognitive computing techniques into Cyber Forensics as presented in this paper. However, we highly acknowledge the contribution made by the above-mentioned authors. The next section presents an overview of the proposed framework.

4. Deep learning cyber-forensics (DLCF) framework

As a contribution into the field of cyber forensics, this section presents a framework for diverging deep learning cognitive computing techniques into cyber forensics here after referred to as the DLCF framework. The goal of the DLCF framework is to show the abilities and capabilities that DL can bring into the field of cyber forensics. This framework is explained using diagrams at a more generic level as shown by Figs. 2–4 in the sections to follow. Being a generic framework the details of the deep learning algorithms are not discussed in details in this paper except where specific examples are given. Fig. 2 represents the high-level view of the framework while Fig. 3 shows the different phases of the framework and finally Fig. 4 represents the detailed framework of all the proposed phases.

4.1. High-level view of the DLCF framework

The high-level view of the proposed framework is organized into five layers labelled 1 to 5 as shown in Fig. 2. The layers include: Initialization Process, Potential Digital Evidence (PDE) Data Sources Identification, Deep Learning Enabled Cyber Forensic Investigation Engine, Forensic Reporting and Presentation, and finally Decision Making and Case Closure.

Each of the highlighted individual layers in Fig. 2 has been explained in detail using Fig. 3 in the sub-sections to follow. Note that the Deep Learning Enabled Cyber Forensic Engine is further divided into four different phases as shown in Fig. 3. This layer is labelled 3 and is explained separately using a detailed diagram in Fig. 4.

4.1.1. Initialization Process

This process as shown in Fig. 3 is the starting point of the digital investigation process and handles the first response of the incident. The initialization process thus deals with the procedures of initiating an investigation whenever an incident is detected. This is mostly a post-event response mechanism and includes first response after incident detection, planning and preparing a digital investigation process. Because of the nature of the activities involved in this layer, machine learning techniques can be appropriate for planning and scheduling the first responders' tasks. For example, dimension reduction algorithms can be employed to reduce the number of variables a first responder has to consider before finding the exact evidence information required. This will help solve the incomplete or inconsistency of manual activities at this stage which eventually makes the execution of the planned tasks very difficult.

4.1.2. PDE Data Sources Identification

As stated by Ref. [26], in the case of a cybercrime, there exist different types of PDE that can be captured. However, capturing evidence from an unreliable data sources can make it hard for such PDE to be considered for inclusion in any legal argument leave alone for the forensic analysis process itself. For this reason, it is important that investigators identify reliable sources and/or the origin of each of the different types of PDE at hand before the analysis process begins. In this paper as mentioned earlier, it is worth noting also that the forensic data sources may include but not limited to: all digital devices, social media, internet search engines, e-commerce platforms, online cinemas, video footage, smart sensors among other sources. The absence of PDE data

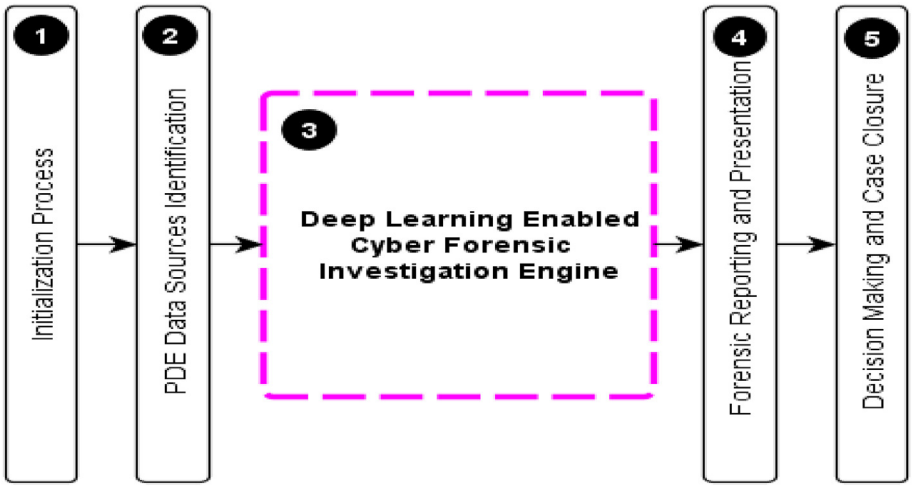

Fig. 2. High level view of the proposed DLCF framework.

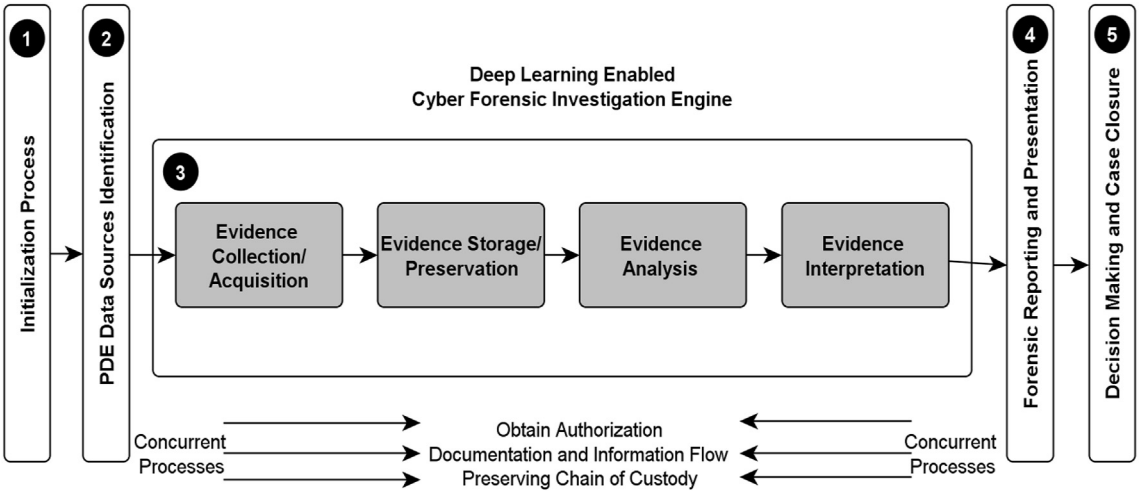

Fig. 3. Phases of the deep leaning enabled cyber forensic investigation process.

sources my complicate the evidence analysis process.

This stage can benefit from clustering techniques, which can be used to find patterns amongst evidence from different records. This is backed up by the fact that, clustering algorithms have the power to group sets of similar data based on defined criteria. It can also allow segmentation of evidence data into several groups and performing analysis on each data set to find matching patterns. Such algorithms can also help determine, for example, the existence of relationships between different available data sources as well as identify the reliability of evidence data sources.

4.1.3. Deep learning enabled cyber forensic investigation engine

This layer is meant to handle the *Investigative Process*. The phases integrated in this layer include: evidence acquisition, evidence preservation, evidence analysis and finally evidence interpretation. Based on the [27]; the evidence acquisition process is concerned with gathering PDE. In most cases, the acquisition process starts with the collection of the most fragile or most easily lost evidence. In some instances, special consideration is also given to evidence or objects which need to be moved into a location away from the crime scene. This is then followed by evidence preservation which has been deemed as one of the extremely important tasks in any investigation process.

However, investigators need to observe all the evidence preservation protocols, depending on the type of evidence at hand before analysis begins. The evidence analysis process is considered a complex process and is meant to provide easiness for digital forensic experts as well as helps jurists' in making accurate decisions. Decision may however be based on how the evidence was interpreted. The evidence interpretation is often required to ensure the evidential weight of recovered digital evidence is clear to all parties involved. Anyone assigned with the task of evidence interpretation after analysis must be competent to do so and be one with sufficient training and knowledge to undertake this task. This *Investigative Process layer* is where the DL algorithms play a major role. Whatever the choice of algorithms used, they are basically meant to have the ability to handle evidence acquisition, evidence preservation, evidence analysis and finally evidence interpretation which is explained in details in section 4.2.

4.1.4. Forensic Reporting and Presentation

Once the *Investigative Process* is complete, a forensic report is inevitable. This report is what is then presented to the different stakeholders. This layer can benefit from classification algorithms.

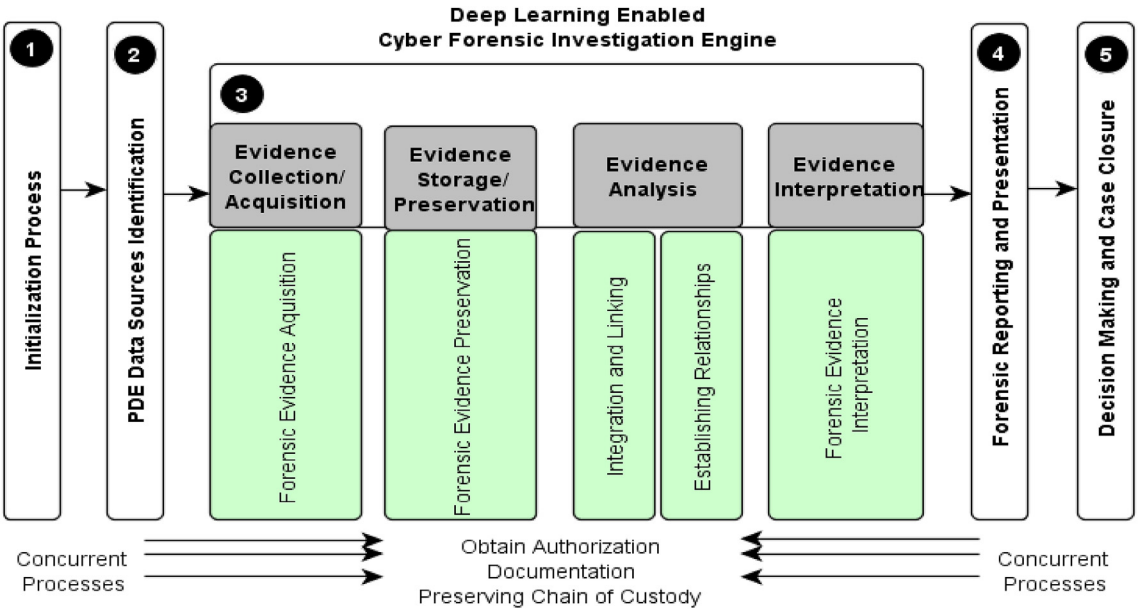

Fig. 4. All-inclusive view of the Proposed DLCF Framework.

This is because, in classification the algorithms have the ability to draw a conclusion from observed values and determine to what category new observations belong. Allowing DL algorithms to assist in producing the forensic report can help save time and money. The forensic report should be such that it is comprehensive and admissible for presentation in any court of law or legal proceedings. In the case of this paper, the report may include but not limited to:

- A detailed analysis of all the PDE captured.
- Proof and justification of all sources of each captured item of the evidence.
- A detailed descriptions of each captured item of evidence and how it was preserved
- Links and relationships that exist between sources and evidence captured
- Detailed descriptions of the intentions of the attacker to the targeted victims
- Explanations on the effects of the attack to the targeted victims
- And any other relevant information to the investigation at hand

4.1.5. Decision making and case closure

Finally, the last layer handles decision making and case closure. This phase is not automated as decisions are to be made by either the jury or any law enforcements agencies based on existing reports. The jury and the law enforcement agencies in most cases are human beings hence the inability to fully automate this phase. Based on the investigation findings as presented in the forensic report, this step may also include information supporting or refuting some hypothesis presented or made in the report or during investigation.

More details of the deep learning enabled cyber forensic investigation engine are explained using an all-inclusive and detailed view of the proposed DLCF framework as shown in Fig. 4.

4.2. All-inclusive detailed DLCF framework

In this section the authors present an all-inclusive detailed DLCF framework which is an extension of the initially presented high-level framework shown in Figs. 2 and 3. In this section however, the focus is made on the Deep Learning Enabled Cyber Forensic Investigation Engine only labelled 3 in Fig. 3. This is because the other layers remain as explained earlier on. The details of the phases under the deep learning enabled cyber forensic investigation engine are thus as explained in the sub-sections to follow.

4.2.1. Evidence collection/acquisition

This layer is intended to handle forensic evidence acquisition as shown in Fig. 4. With the increased volumes of data, forensic evidence acquisition has become a challenging task. Different methods are employed not only to access a potential evidence source but also the type of evidence acquisition that can be undertaken. This implies that one has to have a clear understanding of the manner and type of acquisition that can be done. To reduce errors in acquisition, data mining algorithms can be used to dig deep into data and extract specific artefacts based on a specific criterion. Besides, association algorithms can also be used to discover the probability of the co-occurrence of evidence data within Big Data sources. This is because such algorithms are better at applying models on large data without tiring or complaining of repetitive tasks. However, one must note that any DL algorithm implemented at this point should be such that it can acquire the original digital evidence in a manner that protects and preserves its integrity. This is because, by its very nature, digital evidence is fragile and can be altered, damaged, or destroyed by improper handling.

4.2.2. Evidence storage/preservation

In this layer the main aim is to deal with the way evidence is stored or preserved. Forensic evidence preservation is critical in all forensic investigations, more especially in an investigation that may result in criminal charges. This is because; well preserved evidence can help investigators and law enforcement agents especially when the actions of the first responder may be subject to reviews. Therefore, forensic evidence preservation should be the top priority of those entrusted with gathering and collecting evidence. If evidence is not properly preserved, it may be contaminated or destroyed especially when manual intervention are

involved as many unintended errors can be introduced. In addition evidence not properly preserved prior to forensic analysis may deteriorate, destroying or devaluing it as a source of information [28].

For this reason automating this process with the help of DL algorithms can save an investigator from unnecessary human errors. The DL algorithms used in this layer should be such that they cannot change or alter the PDE as well as employ a variety of evidence preservation protocols up to and until when the investigation is over. This though depends on the type of evidence being analysed.

4.2.3. Evidence analysis

As described by Ref. [29], analysis of the PDE involves the use of a large number of techniques to identify digital evidence, reconstruct the evidence if needed and interpret it, in order to make a hypothesis on how the incident occurred, what its exact characteristics are and who is to be held responsible. This makes evidence analysis to be a very complex process. With the use of Deep Leaning algorithms such as Classification, Prediction as well as the "K nearest neighbours" the complexity of the entire process can be reduced to manageable levels by allowing machines to interact with the evidence. In addition, classification and/or regression can also be used, for example, in spam filtering as well as fraud detection. The outcome of the analysis process should be such that it is relevant, timely, high-quality, and understandable by the different stakeholders. This process also allows for evidence integration and linking as well as establishing relationships using the DL algorithms.

4.2.3.1. Integration and linking. Integration and linking between the available evidence can reveal existing relationships between the evidence and the attacker or targeted victim. Based on the crime committed it is possible that some of the digital evidence captured may have little or no links to either the attacker or the targeted victim. With the help of DL algorithms such as clustering and classification, it is possible to draw these links automatically based on the weight, validity, reliability and the inferences drawn from the PDE itself.

4.2.3.2. Establishing relationships. In the end it should be possible for investigators to establish existing relationships between the PDE with the crime scene. This in most cases reveals any links between the captured evidence and the crime committed. Allowing classification algorithms to handle this process automatically will also help reduce human errors as well as save time and money during forensic investigations. This layer may also be used to find relationships between any captured PDE with other evidence or previously captured evidence.

4.2.4. Evidence interpretation

For any investigator to realise any value from availed PDE, its interpretation becomes very crucial. This backed up by the fact that, accurate interpretation of forensic evidence adds value to the investigation process and assists the court. Thus, DL has the potential to dramatically change the way investigators interpret evidence using algorithms such as classification, clustering among others and provide solutions to cybercrimes.

4.2.5. Concurrent processes

As stated in the [27], this part is meant to handle the processes that should be applied throughout the investigation process. This is because; such processes are applicable to many other areas during an investigation process. Such processes may not necessarily be automated but play a very important role in the entire investigation process. This is captured by Ref. [30] in their paper that documentation as a concurrent process is applicable to all processes within the digital forensic investigation process, since all tasks carried out during the entire investigation process should be thoroughly documented.

5. Conclusion and future work

In this paper, the authors have discussed the concepts of diverging Deep Learning Cognitive Computing Techniques into Cyber Forensics. The authors presented this using the DLCF framework described in Section 4. With the current trends of innovative technologies, new ways and techniques will always be needed to deal with different incidences. It is, therefore, important to build frameworks with the capability to help in forensic investigations as well as support the forensic community. DL has been employed in many disciplines hence the need to incorporate it to Cyber Forensics as well.

Finally, having pointed out the details of the DLCF framework, this research therefore, mentions future work that will involve the development of a prototype that can possible automates some if not all of the different phases mentioned in the proposed framework with the help of DL algorithms. The focus of this prototype will be on how DL cognitive computing techniques can be used to help digital forensic investigators to manage the investigation process. More research also needs to be conducted to improve the DLCF framework proposed in this paper as well as spark further discussion on the development of new digital forensic techniques.

Conflicts of interest

None.

Acknowledgements

The Authors would like to thank the anonymous reviewers that gave constructive review of this paper. Secondly, we gratefully acknowledge the support of the Cyber Security and Forensics Research Group, University of Eswatini, Eswatini; Information and Computer Security Architectures (ICSA) Research group, DigiFORs Research , University of Pretoria; South Africa and the Internet of Things and People (IoTaP) Research Center, Malmo University, Sweden for support while coming up with this research paper. It is worth noting that any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Research Groups and the Universities mention here.

References

[1] P. Hudson, Why the tech revolution is the industrial revolution of our time, Available at: https://www.elitedaily.com/news/technology/tech-revolution-industrial-revolution-time, 2013. (Accessed 15 February 2019).
[2] M. Kaufman, The internet revolution is the new industrial revolution, Avatlable at, https://www.forbes.com/sites/michakaufman/2012/10/05/the-internet-revolution-is-the-new-industrial-revolution/#22b4783447d5, 2012. (Accessed 15 February 2019).
[3] L. Wiegel, Perception in the Digital Age. Analysing Aesthetic Awareness of Changing Modes of Perception, Utrecht University, 2010. RMA Thesis.
[4] T. Young, D. Hazarika, S. Poria, E. Cambria, Recent trends in deep learning based natural language processing, Available at, https://arxiv.org/pdf/1708.02709.pdf, 2017. (Accessed 15 February 2019).
[5] M. Mohammadi, A. Al-Fuqaha, S. Sorour, M. Guizani, Deep Learning for IoT Big Data and Streaming Analytics: A Survey, IEEE Communications Surveys & Tutorials, 2018.
[6] V.R. Kebande, N.M. Karie, H.S. Venter, A generic Digital Forensic Readiness model for BYOD using honeypot technology, in: 2016 IST-Africa Week Conference, 2016, pp. 1–12.
[7] Y. Zhang, Y. Lin, Research on the key technology of secure computer forensics,

in: 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, 2010, pp. 649–652.
[8] L. Nodarishvili, Is cyberspace a new war domain?, Available at, https://digi.lib.ttu.ee/i/file.php?DLID=11279&t=1.Research.Thesis, 2018. (Accessed 15 February 2019).
[9] A. Papanikolaou, V. Vlachos, A. Papathanasiou, K. Chaikalis, M. Dimou, M. Karadimou, November). Cybercrime in Greece: how bad is it?, in: Telecommunications Forum (TELFOR), 2013 21st IEEE, 2013, pp. 1–4.
[10] Hackmageddon, February 2018 cyber attacks statistics. https://www.hackmageddon.com/2018/04/06/february-2018-cyber-attacks-statistics/, 2018.
[11] Comparitech, Terrifying cybercrime and cybersecurity statistics & trends [2018 EDITION]. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref, 2018.
[12] Microsoft, Available at, https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics, 2018.
[13] B. Sahu, N. Sahu, S.K. Sahu, P. Sahu, April). Identify uncertainty of cyber crime and cyber laws, in: Communication Systems and Network Technologies (CSNT), 2013 International Conference on, IEEE, 2013, pp. 450–452.
[14] M. Chaturvedi, A. Unal, P. Aggarwal, S. Bahl, S. Malik, June). International cooperation in cyber space to combat cyber-crime and terrorism, in: Norbert Wiener in the 21st Century (21CW), 2014 IEEE Conference on, IEEE, 2014, pp. 1–4.
[15] M.A. Khan, S.K. Pradhan, H. Fatima, March). Applying data mining techniques in cyber crimes, in: Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on, IEEE, 2017, pp. 213–216.
[16] T. Ling, June). The study of computer forensics on linux, in: Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on, IEEE, 2013, pp. 294–297.
[17] C.H. Yang, P.H. Yen, Fast deployment of computer forensics with USBs, in: Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on, IEEE, 2010, November, pp. 413–416.
[18] M.A. Abbas, March). Improving deep learning performance using random forest HTM cortical learning algorithm, in: Deep and Representation Learning (IWDRL), 2018 First International Workshop on, IEEE, 2018, pp. 13–18.
[19] J. Wu, Y. Yu, C. Huang, K. Yu, Deep multiple instance learning for image classification and auto-annotation, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 3460–3469.
[20] A. Majumdar, V. Singhal, Noisy deep dictionary learning: application to Alzheimer's Disease classification, in: Neural Networks (IJCNN), 2017 International Joint Conference on, IEEE, 2017, May, pp. 2679–2683.
[21] J. Wang, D. Pei, "Kernel-based deep learning for intelligent data analysis," 2017, in: First International Conference on Electronics Instrumentation & Information Systems (EIIS), Harbin, 2017, 2017, pp. 1–5.
[22] D. Ariu, G. Giacinto, F. Roli, Machine Learning in Computer Forensics (And the Lessons Learned from Machine Learning in Computer Security). AISec'11, October 21, 2011, Chicago, Illinois, USA, 2011.
[23] P. Bhatt, P.H. Rughani, Machine learning forensics: a new branch of digital forensics, Int. J. Adv. Res. Comput. Sci. 8 (8) (2017) 217–222.
[24] S. Dilek, H. Çakır, M. Aydın, Applications of artificial intelligence techniques to combating cyber crimes: a review, Int. J. Artif. Intell. Appl. (IJAIA) 6 (1) (2015) 21–39.
[25] F. Mitchell, The use of artificial intelligence in digital forensics: an introduction, in: Proceedings of the 2nd Conference on Advances in Computer Security and Forensics, Liverpool John Moores University, School of Computing & Mathematical Sciences, 2010, 2007.
[26] Karie, Venter, Towards a framework for enhancing potential digital evidence presentation, in: Proceedings of the Information Security for South Africa, 2013. Johannesburg, South Africa, 2013.
[27] ISO/IEC 27043, Information Technology – Security Techniques – Incident Investigation Principles and Processes, 2015.
[28] K.J. Mahoney, Collecting evidence and preserving evidence, available at, https://www.relentlessdefense.com/forensics/preserving-collecting-evidence/, 2014. (Accessed 27 November 2018).
[29] A. Valjarevic, H.S. Venter, Harmonised Digital Forensic Investigation Process Model. " 2012 Information Security for South Africa, Gauteng, Johannesburg, 2012, pp. 1–10, https://doi.org/10.1109/ISSA.2012.6320441, 2012.
[30] A. Valjarevic, H.S. Venter, Introduction of concurrent processes into the digital forensic investigation process, Aust. J. Forensic Sci. 48 (3) (2016) 339–357.