Emerging trends in Digital Forensic and Cyber security- An Overview

Bhoopesh Kumar Sharma
Department of Forensic Science
Amity University Dubai, UAE
bsharma@amityuniversity.ae

Michelle Ann Joseph
Department of Forensic Science
Amity University Dubai, UAE
michelleJ@amitydubai.ae

Mr. Biju Jacob
Director-Business Development
Digital Insight Dubai, UAE
biju@dicuae.com

Lt. Col. Bryan Miranda
Director and Cyber expert,
Digital Insight Dubai, UAE
bryan@dicuae.com

Abstract: **Digital forensics is the application of forensic and scientific knowledge to retrieve information legally from any digital device such as computers and smartphones. This legally fetched information is then presented as a piece of evidence in the courtroom further. Computer forensics also refers to digital forensics. It is the fusion of domains such as network forensics, server forensics, computer forensics, internet forensics, social media forensics, memory forensics, online gaming, data/disk forensics, and VR forensics. While investigating digital crimes, different steps are involved. These include the identification, recovery, investigation, validation, and presentation of evidence.**
Recent research has demonstrated the immense succession of cyber threats and attacks, requiring forensic experts and forensic scientists to simplify the digital world system. Since digital forensics is straightforwardly interconnected to data recovery and data carving, this area is dealing with different technical, legal, and resource challenges. In contrast to that, malware's constant rise allows forensic sector slacking. The objective of the present study was to explore new dimensions of digital forensics such as internet forensics, social media forensics, and IoT forensics in various emerging fields. Together, all our findings allow a better understanding of digital forensics, which can be helpful in forensic investigation.

Keywords: Digital forensic, computer forensic, cyberattack, approaches, social media forensics, malware.

I. INTRODUCTION

For the analysis of pieces of evidence found in one or more digital devices, digital forensics applies scientific methods to explain and recreate the sequence of events that must have occurred in the creation of such artifacts. Digital forensics aims at collecting, reviewing, evaluating, and eventually recording these items and the recorded sequence of events as evidence in the court of law. In a world powered by social networks, the technological evolution comes with the advancement of cyber-crime, which continually creates new kinds of threats, attacks, tools, and techniques that allow offenders to penetrate more complicated or well-controlled environments, cause increased harm, and even remain untraceable. Due to this, organizations are under constant attack from an ever-increasing number of malware spreads at higher rates than ever before. There was no shortage of disruption induced to a worldwide organization, ranging from substantial information breaches and crippling ransomware assaults to a massive increase in cryptojackers.

In 2015, Lloyd's British insurance company estimated that only cyber-attacks to the several companies cost as much as $400 billion in a year, including undeviating damage and post-attack disruption to the standard business path [1]. KPMG's recent cybercrime analysis estimated that 72% of Indian companies were subjected to cyber-attacks in 2016, followed by approximately 63% of economic losses and about 55% of sensual information stolen, resulting in 49% reputational damage [2]. In conjunction with McAfee, the 2018 Strategic and International Studies Research Center (CSIS) reports that about $600 billion, almost one percent of global GDP, is lost to cybercrime annually [3]. Indeed, cloud computing, social media, gaming, virtual reality, and the Internet of Things were among the newest technologies in the field. This paper focuses and provides information on latest trends in cyber threats, new domains in digital forensics, and eventually concludes the challenges faced by forensic investigators during criminal investigations.

The remaining part of the study is structured as follows: Section II briefly presents trending cyberattacks targeting organizations, while Section III discusses the new domains of digital forensics and the challenges faced by forensic

experts in investigating these new areas. We conclude the paper in the last section by suggesting ways to overcome the challenges faced by forensic experts.

II. BACKGROUND

In this section, we have provided a comprehensive overview of the trends observed in the categories of Crypto miners, Ransomware, Malware techniques, Data Breaches, Mobile and Nation-State cyberattacks, and their targets.

A. RANSOMWARE ATTACKS

Ransomware is defined as a malware that usually encodes or deletes networked computer data, traps information, and makes it inaccessible and unusable. It is recognized as a significant threat to computer and network security worldwide and has emerged as one of the most dangerous cyber threats in latest years, with extensive damage. Recent research suggests that ransomware appears as a severe threat and challenge for home users, healthcare systems, and information security professionals and organizations. Even payment does not ensure the release of encrypted records, and likewise, decrypted files do not imply the removal of malware from the system [4]. Ransomware typically targets all types of file extensions without any barrier. Knowing that such files are potentially essential to the sufferers, the attacker encrypts these files, making it much more challenging for the victim to access them. So, to avoid being a victim of ransomware attacks, preventive measures should be taken regularly to back up relevant data and files.

B. BOTNETS

Botnet is remotely controlled set of computers by assailants (botmaster) through a network of command and control without their owners ' knowledge. Botnets are used to conduct multiple malicious operations such as a distributed denial of service attacks, click fraud, sending spams emails to host phishing sites, etc. The major difference between the botnet in comparison to other types of attacks is the presence of Command-&- Control that works in giving orders from botmaster to bot. Bots also hide when the bot detects the target they send to the botmaster in search of an unattended target [5]. It takes a high level of internet privacy and security knowledge to stop a network device from falling victim to a botnet.

C. CRYPTO MINING ATTACKS

Botnet is remotely controlled set of computers by assailants (botmaster) through a network of command and control without their owners ' knowledge. Botnets are used to conduct multiple malicious operations such as a distributed denial of service attacks, click fraud, sending spams emails to host phishing sites, etc. The major difference between the botnet in comparison to other types of attacks is the presence of Command-&- Control that works in giving orders from botmaster to bot. Bots also hide when the bot detects the target they send to the botmaster in search of an unattended target [5]. It takes a high level of internet privacy and security knowledge to stop a network device from falling victim to a botnet.

III. NEW EDGES IN DIGTAL FORENISCS

A. IOT FORENSICS

The Internet of Things (IoT) is a new paradigm that gains ground exponentially in the current scenario of mobile telecommunications. On a conceptual level, the internet of things refers to the interconnectivity of our daily devices, together with the independence of the process, sensing power, and situational knowledge. IoT devices mainly include PCs, laptops, tablets, smartphones, Personal Digital Assistance Devices (PDAs), and other portable embedded devices [9]. Contracted Internet of Things (IoT) devices continuous growth has allowed individuals to share data. Such IoT systems can interact with each other directly or through the Internet Application Programming Interface, and can be operated by high-computing devices, such as cloud servers. IoT systems smartness and networking capabilities offer a wide range of advantages for both domestic and business applications. Nonetheless, there are several security attacks and threats to emerging IoT technologies. Notable risks include attacks on ransomware, Denial of Service (DoS) attacks, destruction of the Internet of Things networks, and mass monitoring [10,11].

Therefore, well-trained teams will carry out a digital investigation on the crime scene, known as IoT forensics, to investigate these attacks. However, IOT presents several unique and complex challenges in the field of IOT forensics. IoT-enabled applications consist of a massive number of distinct and resource constrained devices, which produce a massive amount of data called as Big IoT Data [12]. Unlike traditional forensics, where common sources of evidence originate from PCs, smartphones, servers or gateways. Several factors are affecting IoT forensics impacting conventional digital forensics, as described in Fig. 1. According to MacDermott, et al., (2018) the retrieval of massive amount of IOT data will result in an equitable increase in the workloads carried by data centers. This, in turn, will indicate that providers are being forced to face new capacity, security, and analytics challenges. Guaranteeing that these data are managed efficiently is an essential task, as the overall performance of the application depends largely on the properties of the data management system [13]. Similarly, Alenzi et.al., (2019) stated that securing the chain of custody, complexity and diversity of IOT devices, lack of forensic tools and security issues such identity

spoofing, data tampering, obtaining unauthorized access control, Dos attack are the main challenges faced by IOT forensics. Furthermore, forensic experts face numerous challenges while detection, retrieval, analysis and preservation of evidences while employing traditional investigation methods. In conclusion, the final report must present acceptable evidence to the jury [14]

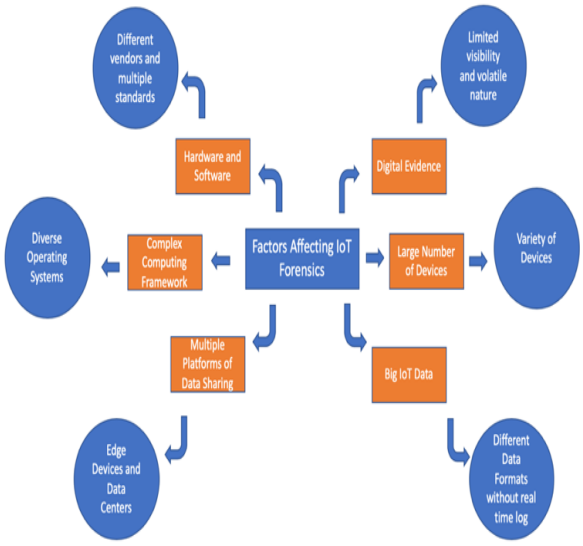

Fig 1. Factors of IoT affecting conventional digital forensics.

The IoT forensics investigation includes a variety of challenges based on non-compliance with the computer forensics methods and traditional forensics methods currently available in IoT settings. Several factors are affecting IoT forensics impacting conventional digital forensics, as described in Fig. 1. Many other factors, such as restricted crime scenes, limitations on service-level contracts, dynamic computer architecture, and standardized hardware and software, make IoT forensics further challenging [13].

B. FORENSICS OF SOCIAL MEDIA

Social Media Forensic is a part of the Network Forensics component. It is seen that in the past, different social sites like Facebook, MySpace, Twitter, LinkedIn, etc. have been subjected to various attacks and threats. Attacks on social networking sites may take place either within the network/system or outside the network. Attacks such as retrieving data about cookies occur within a network where attacks such as Denial of Service (DoS) or DDoS occur outside the system. These sites are undefended to many types of cyberattacks. In addition to these security issues, the most significant concern is the database of the social network website, which is the main target of any attacker [15].

In the criminal investigation system, social media posts can provide excellent assistance to investigators if their potential is adequately explored. A brief overview of the practice of social media data in legal proceedings is stipulated in Fig 2. The Social Media Network is an open source of information about potential witnesses, suspects, and offenders and is also ideal for profiling. It provides a diverse and modern subset of single sources of data, such as text messages, contact lists, photographs, geo-location data, demographic information, etc. Metadata (content-related information) and network data can assist in forensic investigations. Besides, these metadata also help to validate the facts of online social networking. Sensibly identified social media evidence may even help to establish a guilty vs. not guilty judgment.

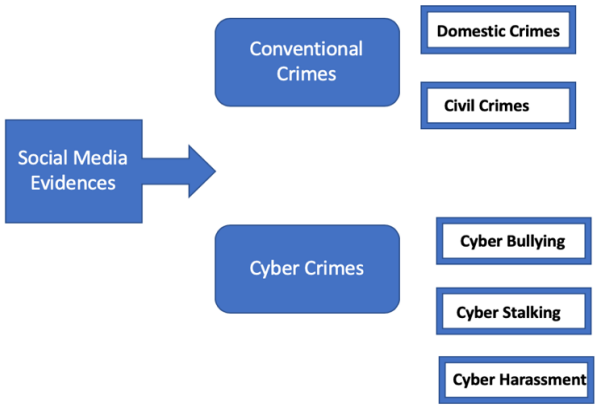

Fig 2. Social media evidence in traditional and cyber crimes.

However, to benefit from data hosted on social media websites, investigators need to address intimidating resources, technological, and legal issues. Firstly, there are the technical challenges; the artifacts might be too complicated to translate into some understandable information. Secondly, legal challenges include the admissibility of evidence and issues related to the collection of data. Evidence from the social channels' platform is un-authenticated, so authentication requires certain collaborating and supporting evidence. The protected privacy rights of the defendant also limit the gathering of evidence from their public platforms [15]. Ultimately, the use of social network outlets in the investigation creates an enormous amount of research for specialists in digital forensics.

A survey conducted by Fahidi et al., (2015) concludes that in order to benefit from data hosted on social media websites, investigators need to address intimidating

resources, technological and legal issues [16]. Firstly, there are the technical challenges; the artifacts might be too complicated to translate into some understandable information. Secondly, legal challenges include the admissibility of evidence in the court of law, and issues related to the collection of data. Evidence from the social channels' platform is un- authenticated, so authentication requires certain collaborating and supporting evidence. The protected privacy rights of the defendant also limit the gathering of evidence from their public platforms. Ultimately, the use of social network outlets in the investigation creates an enormous amount of research for specialists in digital forensics. Therefore, it is important to examine the storage and retention of data and the chain of custody procedures in social media forensics in order to provide more reliable evidence to the trial.

A considerable amount of work has been conducted by numerous researchers [17 – 19] on retrieval of data from various devices and networks. Presently, several techniques and practices are used for data retrieval, where data can be efficaciously extracted [20,21]. And yet preservation and presenting social media evidence as an acceptable evidence in court still remains an issue.

C. CLOUD FORENSICS

Cloud computing has become more prevalent in recent years and is being used to support multiple areas of human life. According to International Data Corporation (IDC), by 2020, cloud services supporting hardware and software, cloud service implementation and management will hit $500 billion, more than three times what it is today [22]. Most organisations and companies move their products across the cloud every day, and this innovation is being considered by a large number of businesses. There are several benefits in switching to cloud infrastructure such as reduced IT cost, scalability, access to automatic updates, business continuity etc. According to EurActive (2011) the key features of cloud computing have substantially reduced IT costs. This leads to the widespread acceptance of cloud computing in various private companies and governments [23]. Major Communication Service Provider (CSPs) have data centers throughout the world in multiple jurisdictions offering cloud services to guarantee service availability and value-effectiveness. These multiple data centers replicate information stored in a particular data center to assure abundance and reduce the chances of single point failure. Yet, security and the ever-increasing number of cyber-crimes in cloud environments are the main obstacles for companies to move their systems to the cloud. Despite the positive effect of the rapid evolution of cloud computing on users, an increasing number of users have also viewed the cloud environment as a malicious field.

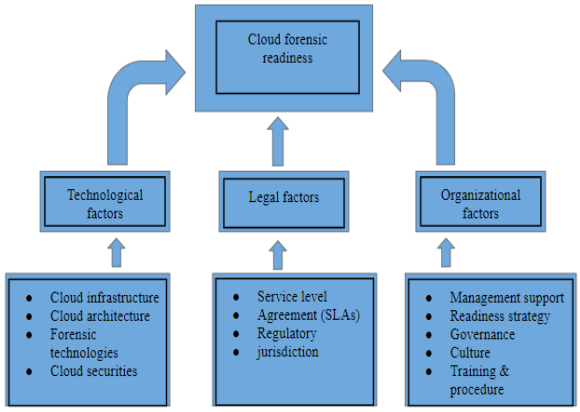

Fig 3: The suggested system for cloud forensic readiness

IV. CONCLUSION

This paper addresses a brief introduction to digital forensics, cyber-attacks, and the continuation of current trends that many experts have identified. The future of digital forensic investigations has been focused on specific tactical capabilities that need to be developed. This paper also deals with the main challenges faced by forensic investigators.

As previously stated, underlying technologies and techniques developed at a tremendous rate. Types of digital devices will continue to differ among devices. Different platforms and storage formats will be used for their shape, structure, component, and communication methods. Media marketing continues to attract user's attention and creativity to upgrades. Likewise, as forensic techniques evolve, improvements in underlying technologies are occurring, specified the swiftness at which the technology is developing. Individuals are quickly turning to methods of contemporary communication tools like social media platforms or modernizing their mobile devices, as stated above. As with other similar sciences, the digital forensic approach is not innovative in nature, but requires constant updating to keep up-to-date and beforehand of current technology instead. The rapid evolution of digital devices requires forensic investigators to use new methodologies and tools to acquire the evidence as legal evidence to be presented in court. As an initial step towards reducing the privacy issues, it is essential to address the root cause of the problem. The solution such problems is in our minds. Educating the human mind to become an ethical person in their work is one of the key factors that we believe will help to reduce privacy concerns. The process of educating people about security must be sufficiently beneficial, as in general we humans tend to explore something new to us. So, no matter how strong computer forensics tools may transform, the privacy of related parties may be jeopardized for the unethical mind, and we need to efficiently create a safe and stable network computing framework that can ensure privacy. Another important point is that, Innovative methods for authenticating

the trustworthiness and validity of digital evidence and meeting scientific and legal standards are also relevant. Therefore, statistical error rates should be measured as far as possible, and specific methods should determine the percentage of confidence. Thus, digital forensic scientists will focus on developing successful test methods and models for gaining scientific validation and legal recognition and approval.

The goal of our paper is to carry out more researches in these areas. Researchers should focus on developing methods that are compatible with the growing legal system. In addition, researchers need to discover new methods in this area for experimental validation and understand the fundamental aspects and complexities of the field due to technological advances and their effect on digital evidence. Hence, our further research will be conducted on tools to retrieve and preserve evidences from these new domains such as social media, IOT and cloud forensics.

REFERENCES

1. "Cyber Crime Costs Projected to Reach $2 Trillion by 2019", *Forbes.com*, 2019. [Online]. Available: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/. [Accessed: 14- Sep- 2019].
2. *Assets.kpmg*, 2019. [Online]. Available: https://assets.kpmg/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf. [Accessed: 14- Sep- 2019].
3. J. Lewis, *Economic impact of cybercrime, no slowing down*.
4. R. Brewer, "Ransomware attacks: detection, prevention and cure", *Network Security*, vol. 2016, no. 9, pp. 5-9, 2016.
5. Hossein, R. Zeidanloo, Azizah, A. Munaf, "Botnet Command and Control Mechanism" 2nd International Conference on Computer and Electrical Engineering, 2009.
6. C. Beek, T. Dunton, S. Grobman, M. Karlton, N. Minihane, C. Palm, E. Peterson, R. Samani, C. Schmugar, R. Sims, D. Sommer, and B. Sun, "Mcafee Threat Report," June 2018.
7. Webroot, "Webroot threat report: Mid-year update," September 2018. [Online]. Available: https:/perma.cc/3M2Z-Q76Y
8. (2013, November). [Online]. vailable: http:/www.ericsson.com/res/docs/2013/ericsson-mobility-report-november2013.pdf
9. Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in Proceedings of the 19th International Conference on Geoinformatics. IEEE, 2011, pp. 1–5.
10. M.M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: World Congress on Services, SERVICES, IEEE, 2015, pp. 21–28.
11. 20. M.A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411
12. Z.A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, et al., Future challenges for smart cities: Cyber-security and digital forensics, Digital Investigation 22 (2017) 3–13.
13. MacDermott, A., Baker, T. and Shi, Q. (2018) 'Iot Forensics: Challenges for the Ioa Era', in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5.
14. Alenezi, Ahmed & Atlam, Hany & Alsagri, Reem & Alassafi, Madini & Wills, Gary. (2019). IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions. 10.5220/0007905401060115.
15. B. Hay, K. Nance, M. Bishop, "Security Challenges for IaaS Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences – 2011. 1530-1605/11.
16. M. A. Fahdi, N.L. Clarke & S.M. Furnell, "Challenges to Digital Forensics:A Survey of Researchers & Practitioners Attitudes and Opinions", Centre for Security, Communications & Network Research (CSCAN) Plymouth University, Drake Circus, Plymouth, United Kingdom info@cscan.org.
17. M. Bader and I. Baggili, "iPhone 3GS forensics: logical analysis using apple iTunes backup utility," Small Scale Digital Device Forensics Journal, vol. 4, no. 1, pp. 1-15, 2010.
18. J. Lessard and G. Kessler, "Android forensics: simplifying cell phone examinations," Small Scale Digital Device Forensics Journal, vol. 4, no. 1, pp. 1-12, 2010.
19. D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, "Network and device forensic analysis of android social-messaging applications," Digital Investigation, vol. 14, pp. S77-S84, 2015.
20. M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, and E. Weippl, "Social snapshots: digital forensics for online social networks," in Proceedings of the 27th Annual Computer Security Applications Conference, Orlando, FL, 2011, pp. 113-122.
21. M. Mulazzani, M. Huber, and E. Weippl, "Social network forensics: tapping the data pool of social networks," in Proceedings of the 8th Annual IFIP Working Group, Pretoria, South Africa, 2012, pp. 1-20.
22. 29. Kohn MD, Eloff Mariki M, Eloff Jan HP. Integrateddigital forensic process model. Computers & Security2013; 38:103–115
23. EurActiv (2011) Cloud computing: A legal maze for Europe. EurActiv February 11.
24. D. Quick and K. K. R. Choo, "Forensic collection of cloud storage data: does the act of collection result in changes to the data or its metadata? Digital Investigation, vol. 10, no. 3, pp. 266-277, 2013.
25. B. Martini and K. K. R. Choo, "Cloud forensic technical challenges and solutions: a snapshot," IEEE Cloud Computing, vol. 1, no. 4, pp. 20-25, 2014.
26. S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," Security and Communication Networks, vol. 9, no. 18, pp. 6285-6314, 2016.
27. Alenezi, A., Atlam, H.F. & Wills, G.B. J Cloud Comp (2019) 8: 11. https:/doi.org/10.1186/s13677-019-0133-z
28. Eecke, P. V. (2015). Cloud Computing Legal is-sues. Retrieved from http:/www.isaca.org/Groups/ProfessionalEnglish/cloudcomputing/GroupDocuments/DLA Cloud%20computing%20legal%20issues.pdf