JISTaP http://www.jistap.org
Journal of Information Science Theory and Practice

RESEARCH PAPER
J Inf Sci Theory Pract 11(4): 14-39, 2023

eISSN : 2287-4577 pISSN : 2287-9099

https://doi.org/10.1633/JISTaP.2023.11.4.2

Digital Forensics Investigation Approaches in Mitigating Cybercrimes: A Review

Abdullahi Aminu Kazaure*
School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
E-mail: aakazaure@student.usm.my

Aman Jantan
School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
E-mail: aman@usm.my

Mohd Najwadi Yusoff
School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
E-mail: najwadi@usm.my

ABSTRACT

Cybercrime is a significant threat to Internet users, involving crimes committed using computers or computer networks. The landscape of cyberspace presents a complex terrain, making the task of tracing the origins of sensitive data a formidable and often elusive endeavor. However, tracing the source of sensitive data in online cyberspace is critically challenging, and detecting cyber-criminals on the other hand remains a time-consuming process, especially in social networks. Cyber-criminals target individuals for financial gain or to cause harm to their assets, resulting in the loss or theft of millions of user data over the past few decades. Forensic professionals play a vital role in conducting successful investigations and acquiring legally acceptable evidence admissible in court proceedings using modern techniques. This study aims to provide an overview of forensic investigation methods for extracting digital evidence from computer systems and mobile devices to combat persistent cybercrime. It also discusses current cybercrime issues and mitigation procedures.

Keywords: cybercrime, digital investigation, forensic investigation, mobile forensics, SM forensics, literature review

Received: December 31, 2022 **Revised:** May 20, 2023
Accepted: June 19, 2023 **Published:** December 30, 2023

***Corresponding Author:** Abdullahi Aminu Kazaure
https://orcid.org/0000-0002-8171-8609
E-mail: aakazaure@student.usm.my

1. INTRODUCTION

1.1. Research Background

In today's networked world, both cybercrime and cybersecurity are interconnected. The development of future IT trends depends on the security of existing networks and online services. It is imperative for the safety and economic development of all countries that cybersecurity measures be strengthened, and that critical infrastructure data be protected. The security of the Internet, and the protection of Internet users, have become an integral part of both the development of new services and the management of running services by governments and other business organizations (Ptaszynski et al., 2017).

According to Grover et al. (2016), national cybersecurity and critical infrastructure protection strategy places a strong emphasis on preventing cybercrime. These laws when enacted should be passed to prevent criminal acts or other issues of information and communication infrastructures, as well as acts that endanger the security of national key infrastructures. Cybersecurity presents global and far-reaching legal, technical, and institutional concerns that can only be met by a well-coordinated strategy that takes into account the roles of numerous players and current efforts while operating within an international framework (Edwards et al., 2018).

1.2. Cybercrime

A crime committed through a computer or computer network is referred to as a cybercrime. However, due to the rising frequency of these occurrences, handling and mitigating cybercrime incidents (CIs) has received considerable scientific interest in recent years. Similarly, the term *cybercrime* is frequently used interchangeably with other criminal activities connected to technology such as cyberterrorism and cyberwarfare, which causes complications (Nisioti et al., 2023). According to Morgan (2020) of Cybersecurity Ventures, worldwide cybercrime expenditures will rise by 15% per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015. This is the largest transfer of economic wealth in history, threatening incentives for innovation and investment.

Moreover, this is increasing the number of disasters that cause harm in a year, which will be more profitable to criminals than the global trade in all major illegal drugs combined. Data damage and destruction, stolen money, loss of productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruptions to normal corporate operations are among the most vulnerable problems caused by this threat (Hill & Swinhoe, 2022). In April 2019, it was revealed that two datasets from Facebook applications had been released to the public. More than 530 million Facebook account details were collected. This data was openly available two years later in April 2021, indicating considerable and actual criminal intent about the data (Pitchkites, 2022).

Data breaches can have devastating effects on hundreds of millions, if not billions, of people. The extent of data breaches has expanded in tandem with the rise of digital technology as cyber-criminals take advantage of people's increasing reliance on electronic information. One of the cyberattacks that knocked down the Yahoo server in 2016 was suspected to have been carried out by a hacker group. These hackers were reported to have gained access to the account information of more than a billion Yahoo users as the company was being acquired by Verizon (Hill & Swinhoe, 2022). However, about three billion Yahoo user accounts were compromised less than a year later. In 2020, the Internet Crime Complaint Center (IC3) of the FBI had its busiest year combating cybercrime, with a record number of Americans reporting being victims of cyberattacks. Since the beginning of 2020, the IC3 has witnessed a rise in phishing, spoofing, extortion, business email compromise attacks, and online fraud aimed at those displaced by the coronavirus pandemic (Pitchkites, 2022). In the same year, the IC3 of the FBI received 69% more cybercrime reports than in 2019. The global fight against the 2019 Coronavirus pandemic is continuing, while cybercrime abroad is growing exponentially (Interpol, 2020; Monteith et al., 2021).

1.3. Cybercrime Victimization of Businesses

Data breaches, distributed denial of service (DoS) attacks, phishing, and ransomware attacks are some of the threats that affects businesses who fall victim to cybercriminals. Research on the effects of ransomware and associated complications on data breaches has triggered serious problems, as noted by Agrafiotis et al. (2018). Certain characteristics, actions, and cybersecurity practices inside businesses are associated with a higher risk of being victimized and more severe repercussions (Connolly et al., 2020). However, a thorough knowledge of the fundamental tools and processes used to hunt down cyber-criminals is a crucial aspect of information security, for the simple reason that having expertise in these technologies makes the tasks of security professionals easier and more efficient. Professionals in the security field may enhance their abilities to deter criminal behavior by acquainting themselves with and adapting to a variety of technology and tactics. Understanding these approaches may assist them in extending their perspectives as security professionals using their experiences while using technology across different domains (Baig et al., 2017; Horan & Saiedian, 2021). Similarly, despite these security measures, cybercriminals are always developing new strategies for executing cyberattacks. There are three separate layers of Internet crime, which consist of the "open" or "surface" online, the "deep" web, and the "dark" web. To prevent these criminal acts, investigators must be acquainted with the technologies and tactics that enable them to access and utilize the abundance of information accessible on different platforms including social networks. For instance, investigators may examine information on Bitcoin transactions on the dark web to gain insight into allegations of misconduct (Tymoshenko et al., 2022).

1.4. Research Purpose

The purpose of this study is to explore and analyse existing techniques for preventing and mitigating cybercrime from the researcher's point of view, particularly in the context of the current trend of IT services adoption. The Internet's simplicity, speed, and anonymity have created a new platform for criminals to expand their operations through cybercrime. The introduction of new advanced technologies such as social networks has resulted in cybercriminals implementing new patterns that are more mysterious and damaging to organizations and individuals. Cybercrime causes business owners to lose billions of dollars each year. However, it can take various forms, including financial crimes such as online fraud, abuse, computer attacks, and tolerance or encouragement of unlawful behavior such as gambling, child pornography, and copyright infringement.

1.5. Research Questions

i. What are the common approaches used by cybercriminals in launching their attacks?

ii. Why is cybercrime on the rise, and how can it be prevented?

iii. How prevalent is online crime? And how do forensic investigation techniques help in mitigating this menace?

1.6. Research Objectives

i. To examine and explore the approaches utilized by cybercriminals in carrying out their attacks to exploit individuals.

ii. To propose strategies for preventing cybercrime and implementing effective measures to adequately address it.

iii. To investigate the critical role played by forensic investigation techniques in mitigating cybercrimes.

2. RELATED LITERATURE

The field of cybersecurity known as "digital forensics" examines and recovers data from digital media to confirm or reject a security-related hypothesis. Evidence is carefully collected from digital media stored on digital devices (such as mobile phones and computers) that may have been utilized in criminal conduct (Flores et al., 2021). The significance of digital forensics for the use of digital evidence in the field of forensics science is projected to expand in the coming years. Sunde and Horsman (2021) reaffirm that both cybercriminals and security experts are using technology extensively due to its scalability. Consequently, the significance of cybersecurity and digital forensics cannot be overstated (Bankole et al., 2022). However, it is important to safeguard businesses from cyberattacks, benefit from digital pieces of evidence left behind after an intrusion or any cyberattacks, and be digitally andscientifically prepared for any kind of cyber/digital incident. According to Ariffin and Ahmad (2021), there is a plethora of studies on information security risk management models within the digital forensics domain.

Some forensic frameworks have already been developed for mitigating cybercrime in response to criminal acts committed in cyberspace. These models and frameworks have provided a fundamental base and starting point for further development during and after the forensic investigation process. The existing new framework has been used to refine the conventional framework. In 2001, Lee et al. (2001) presented a scientific crime scene investigation (SCSI) approach to digital forensic investigation. This paradigm provided a basic framework for digital forensic research in the domain. Although Lee et al. (2001)'s model was not developed in the field of digital forensics, it has had a considerable impact on digital forensics process models. In the same vein, Ciardhuáin (2004) criticizes the (SCSI) 2004 model for not providing a systematic digital forensics process, because his approach primarily focuses on physical crime scene investigation and misses some key essential organizational processes. Although Lee et al. (2001)'s criticism does not offer a solution, it does call for a thorough and methodical investigation. Though various models have been developed and specified since 2014, none of these models involve a significant part of the cybercrime investigation.

However, Kohn et al. (2013) presented an integrated digital forensic process model that depicts the physical crime scene investigation approach and can be utilized for digital crime scene investigation. Several studies (Bankole et al., 2022; Dykstra & Sherman, 2013) in digital forensics examine hypothetical, experimental, and simulated security problems, which provides insights for investigation. Similarly, Weiss and Miller (2015), on the other hand, investigated a financial data breach at Target, a United State (US) based supply chain organization. Target lost around $248 million in 2013 as a result of fraudsters stealing financial details (the data breach was discovered in 2013). The Target financial breach report was made public as a consequence of payment system development legislation enacted by the 114th Congress. Adobe, Sony, Home Depot, and JPMorgan Chase are just a few of the many firms that have faced major digital forensics security issues, such as data breaches in which hackers obtained credit card information. Target and other companies have been obliged to retain third-party investigators to undertake digital forensics security incident investigations (Bankole et al., 2022). Most contemporary security approaches are reactive rather than proactive, and as a consequence they do not adequately address forensic and security concerns. Similarly, Spruit and Röling (2014) developed a model of information security maturity that classifies processes into four categories: technical, organizational, and technological, as well as support, organizational, and technical.

However, in a similar work Javed et al. (2022) conducted a comprehensive review of digital forensic techniques used in cybercrime investigations. They found that digital forensic experts employ different techniques such as digital evidence acquisition, data recovery, network forensics, and incident response planning. The authors also stress the importance of specialized skills and expertise for digital forensic experts to effectively combat cybercrimes.

On the other hand, Al-Khater et al. (2020) conducted a comprehensive review of cybercrime detection techniques with digital forensic techniques used in cybercrime investigation and prevention. They found that forensic experts use various techniques including digital evidence acquisition, data recovery, network forensics, and incident response planning. The authors also underscore the significance of collaboration and communication between forensic experts and other stakeholders, such as law enforcement agencies (LEAs), in effectively mitigating cybercrimes. In general, these studies provide valuable insights into the techniques used by forensic experts to mitigate cybercrimes, including digital evidence acquisition, analysis, interpretation, malware analysis, network traffic analysis, incident response planning, and data recovery (Kebande et al., 2020). Furthermore, the studies highlight the importance of continuous education and training for forensic experts, as well as collaboration and communication with other stakeholders to better combat cybercrimes (Javed et al., 2022).

3. CYBERSECURITY THREATS

Cybersecurity threats continue to grow in intensity, variety, and impact despite significant efforts by businesses, governments, and research institutes to address many of these vulnerabilities. Investigating current cybersecurity risks, evaluating the degree to which relevant protections have been implemented, and assessing the success of risk mitigation activities become logical as a result (Al-Khater et al., 2020). To properly address these concerns, extensive empirical data must be gathered and examined using a variety of Internet measuring approaches. Even though such measures may provide thorough and trustworthy insights, doing so involves difficult processes that call for the creation of cutting-edge approaches to guarantee accuracy and thoroughness. To illustrate how the Internet ecosystem was separated into many components, Pour et al. (2023) presented a taxonomy of cybersecurity focused as presented in Fig. 1.

There are several issues that arise from cyberattacks and a lack of cybersecurity concerns. In addition, many do not think cybersecurity is a major issue and hence rarely take precautions (Monteith et al., 2021). Therefore, the users and relevant stakeholders must have a greater understanding of the benefits of cybersecurity solutions. It is critical to protect the privacy of sensitive information stored on one's computer or a company's network. The data stored on computers or hard drives is both sensitive and confidential. In a corporate setting, this information might be used by competitors to bring a target down or perhaps wipe it out entirely. Disclosure of sensitive information might destroy a person financially in their private life. Information that is not meant to be shared publicly must be encrypted using advanced cybersecurity technologies (Al-Khater et al., 2020). Cyberattacks are difficult to manage, and implementing cybersecurity measures proactively reduces costs considerably. Attacks on cyberspace may result in the loss of clients and popularity for large

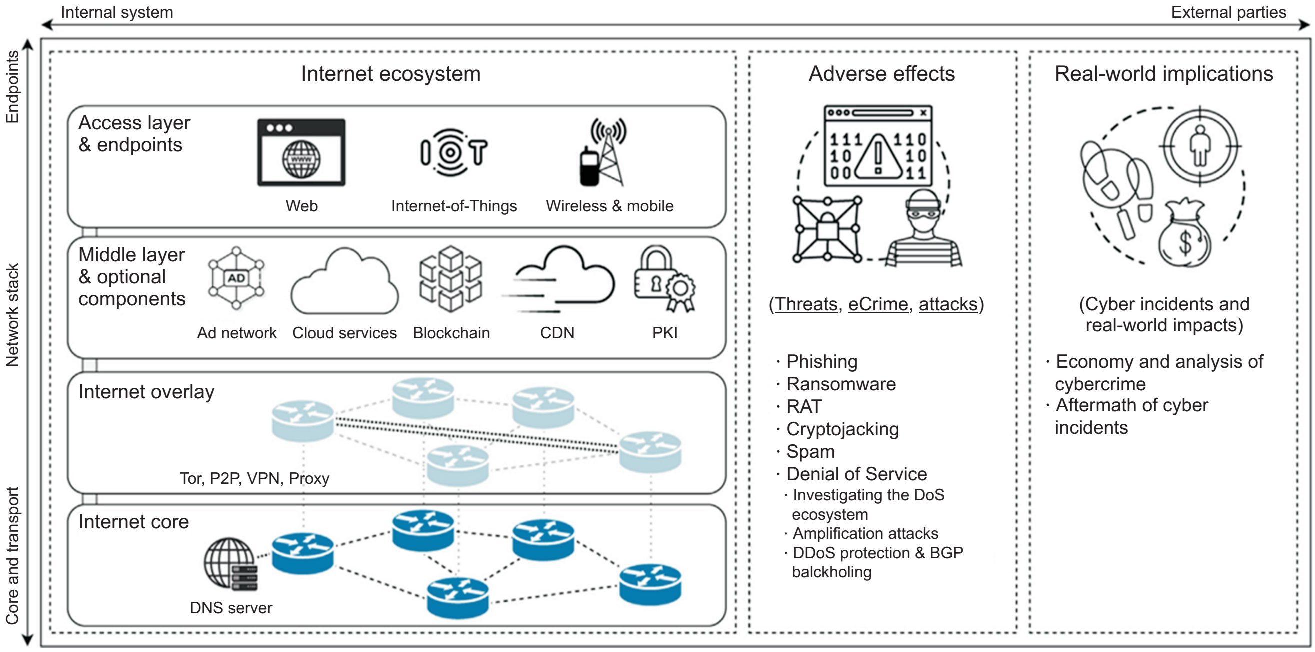

Fig. 1. The Internet ecosystem. Adapted from the article of Pour et al. (Computers & Security, 2023;128:103123). CDN, content delivery network; PKI, public key infrastructure; Tor, the onion router; P2P, peer to peer; VPN, virtual private network; DNS, domain name system; RAT, remote access trojans; DDoS, distributed denial of service; BGP, border gateway protocol.

corporations.

According to Morgan (2020), individuals are an integral part of the cyberspace ecosystem, and when they engage with a business, they may share personal information with the expectation of confidentiality. However, when cyberattacks occur and their information and data are compromised, it erodes customers' trust in the organization, which in turn has a detrimental impact on the company's reputation within the community. The perception of a company by the public plays a significant role in its success, and any damage to its image can result in the loss of customers. Therefore, in cybersecurity, as in other domains, it is better to focus on prevention rather than attempting to restore stability after a system breach. Safeguarding systems proactively is more advantageous than grappling with the aftermath of a malicious intrusion (Tsakalidis et al., 2019).

3.1. Cybersecurity Incidents

A cybersecurity incident refers to an attempt or actual breach of an organization's information security system and it can cause severe consequences for the organization, such as reputational damage and financial loss (Sultan, 2021). One instance of a cybersecurity incident is the Equifax data breach that occurred in 2017. Equifax, a major credit bureau in the United States, experienced a cyberattack that resulted in the exposure of personal data belonging to roughly 143 million individuals. The attackers exploited a flaw in Equifax's website software, which enabled them to obtain unauthorized access to sensitive information like social security numbers, birth dates, and addresses (Bernard et al., 2017). The incident inflicted financial loss and significant harm to Equifax's reputation. Another illustration of a cybersecurity incident is the 2020 SolarWinds supply chain attack. A group thought to be associated with the Russian government conducted the attack by exploiting vulnerability in the software of SolarWinds, a leading provider of network management software. The attackers manipulated the software's code to insert a backdoor, which allowed them to gain access to the systems of SolarWinds' customers, including multiple US government agencies (The White House, 2021). The attack had grave national security implications and led to increased scrutiny of supply chain security in the technology industry.

Generally, cybersecurity incidents are critical threats that can cause severe consequences for both individuals and organizations. The Equifax data breach and SolarWinds supply chain attack demonstrate how cyber-criminals can exploit software and system weaknesses to gain access to sensitive information. Therefore, organizations need to implement effective cybersecurity measures and regularly update their systems to prevent and mitigate the impact of cybersecurity incidents (Sultan, 2021).

According to Tsakalidis et al. (2019), CI Architecture provides a full cybercrime embodiment through feature identification, offense categorization processes, threat severity labeling, and a completely innovative Adaptive Reaction Policy (ARP) that identifies and connects the necessary stakeholders for preventative measures and response activities. The authors designed an architecture consisting of four unique, complementary components that result in a manually made ARP that will in the future be built automatically. The objective is to create a complete platform for the automated management of cybercrime. Fig. 1 depicts the proposed CI Architecture, which consists of four components (I, II, III, and IV). It provides a systematic approach to effective CI management with the objectives of generating insights and patterns about CIs, monitoring and evaluating the threat severity of CIs, and developing actionable and appropriate response policies and guidelines for organizations, individuals, and LEAs. The negative repercussions that these ideas could have in the actual world on various sorts of attacks are another instance. According to Tsakalidis et al. (2019), there has been a rise in the frequency of CIs in recent decades, and this trend is projected to continue. The economic impact of cybercrime has also increased in recent years and is expected to further rise by 2025. As a result, there is a pressing need for substantial enhancements in cybersecurity. In response to this, both national and international organizations have been implementing comprehensive techniques for managing cybersecurity incidents on a larger scale. This can be seen in Fig. 2, which illustrates the classification of these incidents.

3.2. Cybersecurity Challenges

Unfortunately, cyber-criminals have become proficient in turning their illicit activities into lucrative businesses. Sophisticated hacking tools, including those used in zero-day attacks, are readily available on the black market, allowing more people to pose a significant threat to the stability of networks and the overall cyber infrastructure. With the increasing reliance on mobile phones for daily tasks such as banking, office communication, and social media, the vulnerability of mobile networks to manipulation by hackers has also increased (Misra & Arumugam, 2022). This has led to a need for high levels of security, such as voice and facial recognition. The Internet of Things (IoT) has also become a significant target for hackers since they can control all devices through a single access point. Cybersecurity challenges are ongoing and continuously evolving, requiring equally evolving and updated countermeasures. Third-party sellers are also at risk of cyberattacks, which can be challenging to prevent due to the most protected areas being the employees themselves.

There is a significant gap between the level of preparedness and the type of cybersecurity issue at hand, with many businesses being aware of the risks but falling short in their responses. The increasing threat posed by cyber-criminals highlights the importance of taking proactive measures to prevent and mitigate cybersecurity breaches (Maalem Lahcen et al., 2020). Businesses must stay up-to-date with the latest cybersecurity technologies

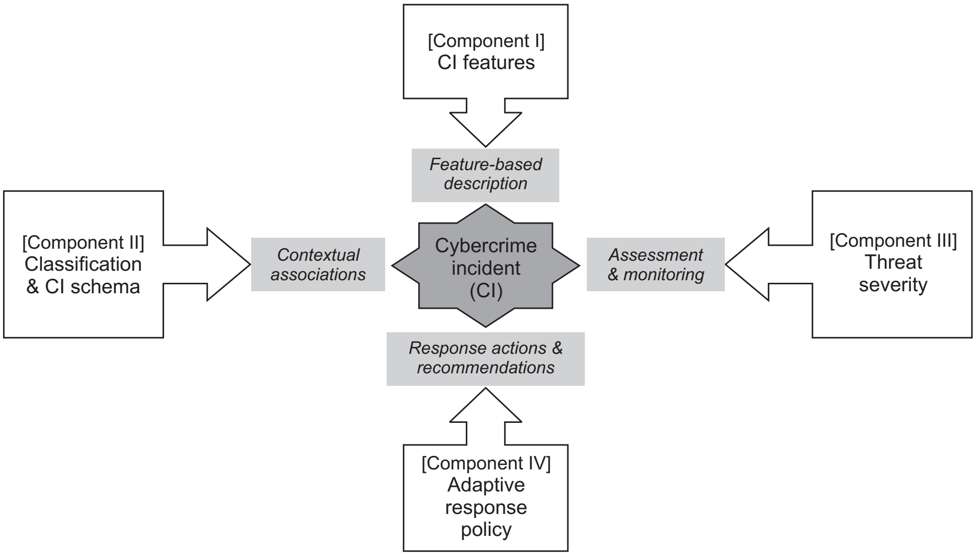

Fig. 2. An overview of the core elements of cybercrime incident architecture. Adapted from the article of Tsakalidis et al. (Computers & Security, 2019;83:22-37).

and techniques to ensure their networks and devices are protected from attacks. They must also take into account the human factor, such as employee training and awareness, to prevent human error from leading to security breaches. It is also crucial for businesses to collaborate with other stakeholders, such as government agencies and security experts, to share information and resources to combat cyber threats effectively. As technology continues to evolve, so do the methods of cyberattacks, and it is crucial to remain vigilant and adaptable in the face of evolving threats (Al-Khater et al., 2020).

4. DIFFERENT TYPES OF CRIMES COMMITTED

There is a wide variety of techniques that criminals use to trick their victims, especially those who have placed their faith in them. In many instances, forensic investigators are called upon to look into how cyber-criminals have used victims for malicious purposes (Al-khateeb et al., 2019). Collaborating with law enforcement and fellow forensic specialists, investigators in forensics strive to unravel the intricacies of a crime. The forensic team usually collects images or creates sketches of crime scenes to documents evidence, collects various forms of evidence such as fingerprints, bodily fluids, and human tissue. Moreover, this data collected can then be analysed in the laboratory. To identify the perpetrator of a crime, it is important to collect and analyse all pertinent physical evidence, which is the essence of forensic investigation (Nisioti et al., 2023).

Money laundering, theft, harassment, and child pornography are all common types of criminal conduct over the Internet (Yeboah-Ofori & Brimicombe, 2018). Online auction fraud, identity theft, financial and telecommunications fraud, credit card fraud, and many more crimes are examples of computer fraud. In the context of computer crime, theft crimes include monetary theft, service theft, data theft, and piracy, and most of these offenses end in allegations of cyber-stalking and cyber harassment (Sun et al., 2021). Child pornographic offenses, like other sexually related crimes, involve both the spread of innocuous material aimed at minors for sexual exploitation and the recruiting of teenagers to conduct sexual actions themselves. The following are some instances of the many types of illegal conduct that cyber-criminals often engage in.

4.1. Cyberstalking

Cyberstalking, in its broadest terms, refers to stalking performed with the use of a computer. Stalking is defined as "persistently harassing and threatening behavior, such as following a person, appearing at a person's house or place of business, making harassing phone calls, leaving notes or things, or vandalizing a person's property" (Arfaj et al., 2022). A cyberstalker is someone who pursues another person in this manner while using a computer. Stalking and harassment are defined as persistent communication via electronic methods (e-mail, instant messaging). In April of 2000, an extraordinary case of cyberstalking occurred in California. According to Nisioti et al. (2023), the defendant of the committed crime pled guilty in this case to charges that he attempted to solicit the rape of a female social acquaintance. However, one of the persons arrested, named Dellapenta, said in online personal advertisements and chat forums that the woman had always fantasized about being raped and played the victim. In his replies to the advertisements, he disclosed the woman's confidential information, including instructions on how to defeat her security system. Six of those who replied to her ad were aggressive and threatened to rape her if they had the chance, or threaten another person. Finally, the FBI and Sheriff worked together to catch Dellapenta. He was found guilty and condemned to jail for six years. However, there are other, less common types of cyberstalking (Dimitriadis et al., 2020). Because it is commonly aimed at persons who have not specifically requested it, spam or unsolicited electronic mail may also be considered a kind of cyberbullying.

4.2. Cyber Terrorism

Cyber terrorism is an illegal act that involves violence against individuals and properties, often driven by political, racial, or ideological motives (Al-Khater et al., 2020). This type of cybercrime often creates fear, anxiety, and violence among people and can also result in sabotage and destruction of properties, such as computers and networks, thereby affecting the availability and integrity of information (Lewis et al., 2017). The Internet is frequently used by terrorists to spread propaganda, recruit individuals, manipulate public opinion, and disrupt national infrastructure, including transportation, dams, traffic lights, and energy facilities. For instance, the Ukrainian attack on a power grid in December 2015, which was initiated with a phishing email, is an example of cyber terrorism (Al-Khater et al., 2020). Certain cyber-terrorist activities instil fear and disrupt citizens, which can also influence political decision-making. The adverse economic effects, property damage, and violence resulting from cyber terrorism can result in fatalities and impact the unity of society (Internet Crime Complaint Center (IC3), 2020).

4.3. Cyberbullying

The increased usage of technology and social media among individuals of varying ages and genders has raised the likelihood of unwanted conduct, such as bullying. Bullying is a highly negative experience, especially during childhood, and is most commonly experienced by children, teenagers, and women. Bullying can cause emotional and mental distress and can impact an individual's character (Lewis et al., 2017). Victims of bullying may receive hostile and offensive tweets, messages, or posts that may include threats of violence or harassment (Nandhini & Sheeba, 2015). Cyberbullying is a form of cybercrime that encompasses activities aimed at causing harm to an individual, including but not limited to identity theft, credit card theft, bullying, stalking, and psychological manipulation (Arfaj et al., 2022). Table 1 outlines some of the different types of cyberbullying that victims may encounter. Table 1 outlines several cyber bullying types that a victim may experience.

4.4. Phishing Attacks

Phishing attacks are a type of online scam in which an attacker poses as a trustworthy entity, such as a bank or a social media platform, to trick a victim into giving up sensitive information like usernames, passwords, credit card numbers, or other personal data (Horan & Saiedian, 2021). Phishing attacks can be delivered via email, text messages, phone calls, or even social media messages. The messages may contain links to fake websites that look like legitimate ones but are designed to steal the victim's login credentials or other sensitive information (Al-Khater et al., 2020). Social engineering and online identity theft, also known as "phishing," occur when malicious actors create fraudulent websites to deceive users into divulging sensitive information. According to the Anti-Phishing Working Group (APWG), there were over 1.2 million unique phishing attempts documented in 2016 alone.

However, one common method employed in these attacks is domain squatting, particularly through typo squatting, where misspelled or slightly altered versions of popular domain names are registered with malicious intent. Another technique involves the use of Internationalized Domain Names (IDNs) to carry out homograph attacks, where visually similar characters from different languages are used to masquerade as well-known domains. The APWG defines phishing as a form of online identity theft that utilizes deceptive emails to redirect individuals to fake websites, tricking them into revealing personal or financial information such as credit card numbers, account credentials, and social security numbers (Nikkel, 2020). Victims may receive an email containing a link to a fraudulent website as part of the phishing scheme. Clicking on the link leads them to a website that appears to be a legitimate platform, like eBay, for example. Despite various mitigation efforts such as email filters, the removal of phishing websites, and the use of browser plugins to warn users about potentially harmful pages, the problem of phishing attacks remains a persistent challenge (Guo et al., 2021).

4.5. Ransomware Attacks

The motive behind widespread ransomware attacks is the expectation of receiving a ransom (Connolly et al., 2020). The objective of ransomware is to block victims' access to their data and demand a ransom payment in return for restoring access (Kolodenker et al., 2017). An end-to-end framework for analysing Bitcoin-based cy-

Table 1. Types of cybercrime

Different types of cybercrime	Nature of the crime usually committed
Cyber verbal abuse	The offender expresses their hatred towards the victim on the victim's social media account
Copying and cloning	The victim's social media profile, which comprises their personal details and photos, is hijacked and private information is acquired
Morphing	The offender retrieves the victim's photograph from their profile and utilizes it for pornographic intentions
Cyber libel	Also referred to as gossip, when the offender tries to disseminate false information about the victim on their social media profile or in online groups
Blackmailing	The offender unlawfully utilizes the victim's personal information obtained from their social media account. Women are particularly susceptible to blackmail and threats, which may include physical intimidation by enemies, ex-spouses, or stalkers

bercrime was developed by Ariffin and Ahmad (2021). From the point at which victims obtained Bitcoins to the point at which the operators cashed them out, the authors tracked all financial activities. The approach for forecasting future ransomware transactions within a ransomware family is novel, efficient, and manageable. The authors found that their method was more accurate than popular heuristic and machine learning (ML)-based approaches. Meanwhile, other authors have developed their methods for detecting ransomware, which led to the development of ground-breaking new techniques. Kolodenker et al. (2017) presented PayBreak as an automated proactive defensive strategy to counter ransomware. This strategy is predicated on the fact that hybrid encryption with symmetric session keys is used for safe file encryption on the target PC. However, the data was recovered from 12 of 20 distinct families of real-world ransomware in tests by PayBreak's authors. Similarly, one way to identify ransomware is by a graph-based technique, as proposed by Moussaileb et al. (2018). Over 700 unique ransomware variants were examined in this analysis of real-world threats. Exploring the file system on a thread-by-thread basis was shown to be enough for detecting malicious applications.

4.6. Online Child Pornography

The term "online child pornography" refers to the distribution of unlawful media involving and directed at adolescents, as well as the sexual exploitation of children by adults who utilize the Internet for this purpose (Akbari et al., 2022). The distribution or possession of child pornography is a federal violation under Title 18 of the United States Code (USC), sections 2252 and 2252A. Furthermore, as mentioned in 47 USC 223, it is prohibited to provide any kind of child pornography to a minor. According to the Business Software Alliance, the FBI's Cyber Crimes Program's Innocent Photos National Initiative is entrusted with investigating crimes like these on a national basis. In certain regions, the FBI collaborates with local law enforcement (Internet Crime Complaint Center (IC3), 2020).

5. DIGITAL FORENSICS

Digital forensics is a branch of forensic science that deals with the recovery and analysis of evidence from digital devices. The primary goal of digital forensics is to identify, recover, and analyse digital content to produce admissible evidence in a court of law (Hargreaves & Patterson, 2012). The use of digital technology has simplified criminal activities, making it easier for criminals to engage in unethical behavior such as tampering with evidence or documents. Digital forensics has emerged as a response to this evolution of crime, and the establishment of the Digital Forensic Research Workshop in 2001 marked the beginning of this field. Initially, the digital forensic investigation was defined as "the application of well-established and scientifically proven procedures for the gathering, identification, and validation of digital evidence that may lead to the reconstruction of criminal incidents" (Mohammad & Alqahtani, 2019). However, as with other scientific disciplines, digital forensics involves the development and testing of hypotheses and models to provide an investigative framework.

However, since its inception, digital forensics has made significant advancements and contributed to the progress of our society. Individuals and organizations are now well aware of the tremendous opportunities presented by this emerging field. With the continuous improvement of criminal methods in the digital realm, there is a growing need for standardized incident-response procedures to address the ever-increasing cyber threats and attacks. When examining digital forensic methods, one crucial aspect revolves around the collection of potential evidence, which serves as a vital artifact (Chuprat et al., 2018). Consequently, investigators involved in digital forensics must possess comprehensive knowledge and expertise in investigative techniques (Karie et al., 2016). Throughout the twentieth century, the popularity of digital forensics has grown significantly due to the widespread adoption and heavy reliance on technology. While traditional forensics defines evidence as physical objects such as blood, fingerprints, or hair that can be used to identify criminals, the concept of "digital evidence" encompasses anything that can be retrieved through digital devices and is associated with digital technology, such as digital files and data. The pivotal role in investigating digital crimes is played by the identification and collection of evidence from diverse sources. In the realm of digital forensics, any pertinent information crucial to criminal convictions is regarded as digital evidence, adhering to the principles of forensic science, and is stored and transmitted digitally as per the requirements (Khanafseh et al., 2019).

The field is also gaining traction with investigators, who have traditionally spent their time focusing on the development of distinctive models for use in digital forensics. Acquisition, identification, evaluation, and admission are the four main stages of the earliest proposed models for digital forensics. Different models have been presented to illustrate the processes required in collecting and analysing information from a broad range of digital devices. According to Karie et al. (2016), digital forensics requires forensic analysts from LEAs to conduct thorough forensic analysis of digital evidence. However, the forensic examination of digital data is equally applicable to litigators and any other legal challenges associated with business organizations.

5.1. Digital Forensics Investigation

Digital forensic investigation is the process of collecting, analysing, and preserving electronic data as evidence in a legal case or investigation (Horsman, 2020). This type of investigation is typically used to identify and gather evidence related to cybercrimes, such as hacking, data breaches, intellectual property theft, and online fraud. The digital forensic investigation process involves several stages (Hemdan & Manjaiah, 2021).

a) Identification: Determine the scope of the investigation and identify the potential sources of digital evidence.

b) Preservation: Secure the digital evidence in a way that ensures its integrity and authenticity, preventing any alteration, deletion, or destruction of the evidence.

c) Collection: Collect the digital evidence using forensically sound techniques such as imaging the hard drives or copying the data from other devices.

d) Analysis: Analyse the digital evidence to identify relevant information, such as the nature of the cyberattack, the attacker's identity, and the extent of the damage caused.

e) Presentation: Present the findings of the investigation clearly and concisely that is admissible in a court of law.

Digital forensic investigations require specialized tools, techniques, and expertise to ensure that the evidence collected is reliable and admissible in court (Kohn et al., 2013). Therefore, it is important to involve experienced digital forensic investigators and legal professionals to ensure that the investigation is conducted properly, and the evidence is presented in a way that meets legal requirements (Marshall, 2021).

The term "digital forensic investigation," or DFI, refers to the process of gathering and analysing digital evidence such as data and files to establish facts for use in legal proceedings. Criminal investigations often include a postmortemexamination of digital evidence using forensic procedures.

Therefore, the results of these investigations might be considered by the court, since they were obtained through scientific procedures and techniques. Since electronic media is too fragile to physically inspect, a tool is normally employed to verify the integrity of the digital data (Hemdan & Manjaiah, 2021). To withstand judicial review, any digital forensic investigation must provide acceptable digital forensic evidence. In general, an investigation aims to discover more about a recent incident (Horsman, 2020). The primary purpose of establishing a potential root cause is to ensure that the investigation can withstand court scrutiny if the situation warrants it. Nevertheless, any investigation must be carried out with caution to guarantee that the investigator's conduct is such that the validity of the evidence supplied cannot be questioned (Marshall, 2021).

5.2. Prospective Digital Evidence

The concept of digital evidence as a distinct element with unique properties and characteristics based on functionality and origin was introduced by Carrier and Spafford (2004). While digital data possesses a physical form, it may not be immediately apparent in computer-based crimes, highlighting the significance of digital evidence for forensic investigators. A reliable framework that ensures the traceability of digital evidence plays a crucial role in detecting potential security incidents, identifying their sources, and understanding their history (Bennett & Diallo, 2018; Lutui, 2016). However, the admissibility, legality, and reliability of digital evidence can vary across countries and require careful examination.

During the examination of digital evidence, it is essential to adhere to fundamental forensic processes, including identification, preservation, acquisition, authentication, and analysis (Turnbull & Randhawa, 2015). Similarly, as the sources of digital evidence have expanded due to advancements in digital technology, investigators must establish reliable sources for each type of digital evidence collected during the investigation. Relying on inaccurate sources of digital evidence can be more detrimental than not using any sources at all, emphasizing the importance of employing scientifically proven methods when collecting potential digital evidence (Casino et al., 2021). However, it is crucial for any scientific procedures utilized in digital forensics to adhere to specific scientific principles and be based on measurable and scientifically established standards (Casino et al., 2021; Horsman, 2018; Javed et al., 2022).

5.3. Digital Evidence Traceability

Digital evidence traceability refers to the ability to track and document the chain of custody and the history of digital evidence, from its creation or acquisition to its presentation in court or other legal proceedings use (Al-Dhaqm et al., 2017). It is a critical component of digital forensics investigations and is essential to ensure the admissibility and reliability of digital evidence in court (Casey & Souvignet, 2020). The traceability of digital evidence requires meticulous documentation and record-keeping at each stage of the investigation, including the collection, preservation, analysis, and presentation of the evidence. This documentation should include the names and contact information of the individuals involved in each stage, the date and time of each activity, and a detailed description of the actions taken, and the tools and techniques used (Turnbull & Randhawa, 2015). Maintaining digital evidence traceability is particularly important in cases where the evidence may be challenged or contested, such as cases involving intellectual property theft, data breaches, or cybercrime. If the chain of custody and history of the evidence cannot be accurately documented and presented in court, the evidence may be deemed inadmissible or less credible, and the case may be compromised (Horsman, 2022).

However, to maintain digital evidence traceability, it is important to follow established protocols and guidelines for digital forensic investigations, including those issued by professional organizations such as the International Association of Computer Investigative Specialists, the National Institute of Standards and Technology (NIST), and the Scientific Working Group on Digital Evidence. These guidelines provide best practices for collecting, preserving, analysing, and presenting digital evidence, including recommendations for documentation and record-keeping to ensure the traceability of evidence throughout the investigation. In today's society, the traceability process has become a crucial component of many aspects of our life, including the digital investigative process.

This is confirmed by Karie et al. (2016), who believedthat traceability may identify occurrences of an event from several sources, assisting in the collection of evidence to be used in a court of law or for any other investigative purposes. The primary purpose of evidence traceability is generally to uncover potential digital evidence and link meaningful connections between the evidence that has been located. Given the origin of an artifact, traceability allows for the tracking of a chain of events as well as the prediction of process outcomes (Casino et al., 2021). As a result, investigators and LEAs may track all components of digital evidence based on its origin and history. The following table shows the evidence traceability guidelines (Table 2).

6. BASIC CHALLENGES IN THE DIGITAL FORENSIC INVESTIGATION PROCESS

There are a variety of difficulties in digital forensics that make it challenging to perform investigations; these obstacles can be categorized as follows.

a) Because digital forensics relies so heavily on evidence obtained from a different variety of digital devices (including laptops, tablets, servers, and cameras), the fact that each of these devices uses a unique data format may cause a significant challenge during processing and analysis.

b) The effectiveness of modern digital forensics tools: While the majority of digital forensics tools were designed to identify a specific piece of evidence, they can also be used for other purposes, like standardizing evidence formats, compressing collected evidence, and extracting crucial information.

Table 2. Evidence traceability

Direct evidence	Circumstantial evidence/ indirect evidence
Physical evidence/real evidence	Scientific evidence
Computer/laptops	Fingerprint identification
Mobile phones	DNA matching
Tablets	Hair and fibre comparison
Modems	Voice identification
iPads	DNA testing
Documentary evidence	Computer generated evidence
Photographs	Output on the monitor (visual)
Letters	Film recorder
Video	Evidence printed on printer
Audio	Evidence printed on plotter
Surveillance tapes	Visual output on the monitor
Printed documents	Charts
Empirical evidence	Criminal confessions
Temperature	Counterfeit money
Checks	Threatening letters

c) The expansion of digital technology in daily life has resulted in a tremendous increase in the volume of data collected from these devices. This enormous amount of data complicates various elements of digital forensic investigations, including the phases of evidence analysis and examination.

d) The format of data obtained from various digital devices necessitates the application of complex data reduction and evaluation techniques.

e) The challenge of building a coherent timeline from many digital sources may involve different time zones, interpret timestamps differently, or suffer from clock skew/drift, among other syntactical discrepancies.

f) One of the primary challenges in digital forensics is a lack of experience and resources, which is why investigators must personally verify the necessity of a specific instrument at various stages of an investigation.

7. DIFFERENT SUB-DOMAINS OF DIGITAL FORENSICS

Digital forensics encompasses several sub-domains that specialize in different areas of investigating and analysing digital evidence. These sub-domains include computer forensics, network forensics, mobile device forensics, memory forensics, forensic data analysis, multimedia forensics, incident response, malware analysis, cloud forensics, and IoT forensics. Each sub-domain focuses on specific aspects such as computer systems, network traffic, mobile devices, memory analysis, data analysis, multimedia files, incident response, malware, cloud environments, and IoT devices. These sub-domains often overlap, and a comprehensive investigation may require expertise from multiple areas. Investigations into crimes that include the use of a digital device as either a tool in the commission of the crime or as a target of the crime is carried out with the help of digital forensics (Choo & Dehghantanha, 2017). As shown in Fig. 3, the field of digital forensics is divided into several subfields.

7.1. Computer Forensics

Digital forensics, or computer forensics, is the application of legal and computer science principles to computer resources to determine the state of a digital artifact, such as a computer system or digital records and other associated information that might assist in the ongoing investigation (Freiling & Schwittay, 2007). To discover evidence of a crime, computer forensics experts investigate digital artifacts such as the data stored on computers and other electronic devices. The time-sensitive nature of digital data means that it must be extracted quickly (Black et al., 2015; Javed et al., 2022). Since the late 1980s, there have been significant advances in the investigation of computer-related crime. Alongside scientific advances, developments in legislation, computer crime classification systems, and digital forensics methodology and theory have been enhanced and shown to be successful. Since digital forensics is still an emerging field, more study and development are required. Even while digital investigative software is rigorously tested to guarantee it is error-free, mistakes can still happen and result in overlooked or misinterpreted evidence.

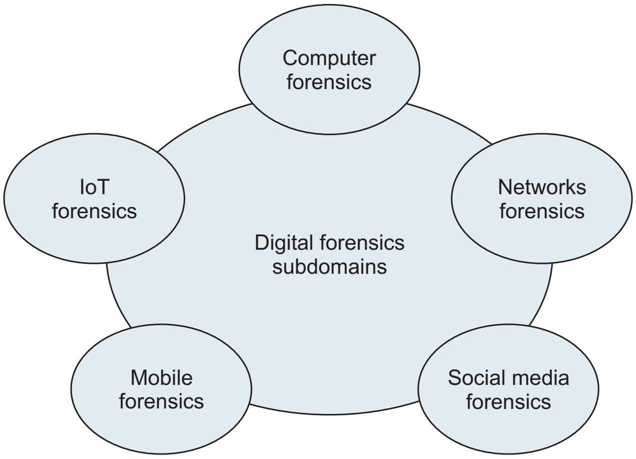

Fig. 3. Digital forensics branches. IoT, Internet of Things.

Digital investigators need to know how to validate their findings to make sure they are correct, and they also need to know which tools are best for a certain task (National Institute of Standards and Technology, 2019). To validate a tool, it must be compared to another tool and its results recorded. This can be done to confirm that the two tools produce consistent results or to guarantee that one instrument correctly understood low-level data. For instance, all tools should reliably derive date-time stamps, and two programs should be able to recover the same deleted data from the same file system. Computer Forensic Tool Testing is a program run by the NIST that can help forensic investigators check the quality of their work and the reliability of their tools (NIST) (Kumar Raju et al., 2016). Forensic tools' ability to acquire digital evidence from storage media and retrieve deleted information is being actively evaluated as part of this endeavor. When performing these tests, we are not attempting to retrieve deleted data using superior gear. By using "spin stand testers," or hard drive testing equipment, some forensic labs can retrieve data that was only partially destroyed (Holt & Bossler, 2015). With this innovation, operators can instruct the read head to retrieve information from the outer portions of a track that has not been overwritten by more recent data recorded in the track's center.

7.2. Network Forensics

Network forensics is a subfield of digital forensics that focuses on detecting and preventing cyberattacks on networks through the analysis and monitoring of network traffic. Network forensics analysis tools may provide services such as network forensics and security investigation, data integrity from many sources, target prediction for future attacks, network traffic analysis, and recording different forms of traffic analysis based on user demands. Here are a few examples of how the network forensics technique may be implemented at various network levels (McCullough et al., 2021). Sniffing tools, also known as monitoring tools, may be used to eavesdrop on bit streams at the Ethernet layer in network forensics, allowing the network forensics process to be completed at this level. Wireshark and the tcpdump are well-known tools for this purpose; tcpdump is especially beneficial for Unix-based computers and can help the investigator collect a variety of evidence at the Ethernet layer.

Internet Protocol (IP) is responsible for transferring transmission control protocol-generated packets across the network by attaching the addresses of their corresponding source and destination nodes (Choo et al., 2017). Every packet traveling from a source node to a sink node must traverse a sequence of routers, each of which maintains a routing table. In network forensics, one type of evidence is the routing tables, which can be used to track the origin of a packet to a specific machine (Javed et al., 2022). When addressing network forensics, the term "additional evidentiary resources" typically refers to the logs maintained by network devices that include information about network activities. Various network device logs can be correlated to reconstruct what transpired during an attack. Due to their limited memory, network devices can be configured to transfer logs to a central server for storage (National Institute of Standards and Technology, 2019).

7.3. IoT Forensics

The use of IoT technologies has recently increased significantly. Smart gadgets are employed in almost every major domain, including healthcare, transportation, smart homes, smart cities, and others (Kebande & Ray, 2016; Nik Zulkipli et al., 2017). However, this technology has several flaws that could lead to cybercrime via the devices. An alternative approach to investigation is required when dealing with crimes using IoT devices because of their alarming frequency (Awasthi et al., 2018). The amount of CIs employing this technology is anticipated to increase, according to Symantec's Internet Security Threat Report 2016.

There is evidence that fraud, ransomware, malicious attacks, node manipulation, phishing, and Structured Querry Language injections are committed utilizing IoT devices and applications, or that devices are used to perpetrate these crimes. Static digital forensics is far more difficult to undertake than conventional computer forensics on these devices because of their network connectivity (Oriwoh et al., 2013; Zawoad & Hasan, 2015). In addition, IoT forensics necessitates real-time investigation because of the limitations of IoT devices and the characteristics of digital evidence that demand proper management (Oriwoh et al., 2013). Fig. 4 depicts the many functions of the IoT environment and their interdependence.

These modules are supported by different processes including storage and timers which display the whole IoT system and how various entities are linked.

i. Sensor Module. Local environmental conditions may be detected and responded to by IoT entities. Sensing modules are classified into two types: controlled sensing and event-driven sensing. The first types detect only when the user or other sensors request the sensor's data at any point during execution (Nik Zulkipli et al., 2017). The latter is called event-driven sensing, and it occurs when

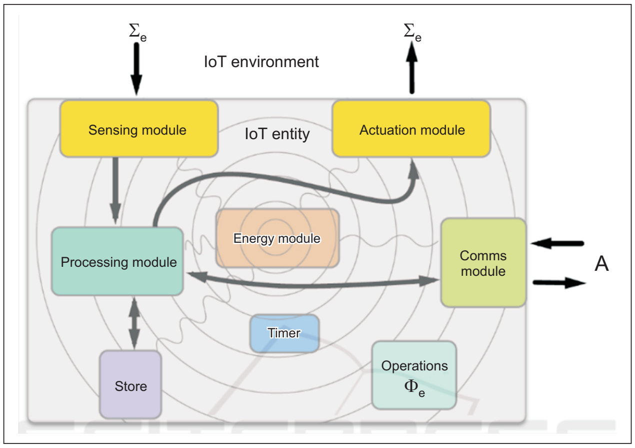

Fig. 4. Internet of Things (IoT) environment operations. A, actuators.

the sensor senses change in its surroundings. The major function of this sensor is to collect and transmit data (or maybe both). The data is subsequently sent to the processing module, which processes it for the next phase. Each sensor in the IoT system requires a unique identifier and physical location to be identified and communicated with.

ii. The Module for Processing. This module is the IoT system's heart, serving as the local brain for the whole system of sensors and applications. The major function is to evaluate and transmit sensor data and information (Nik Zulkipli et al., 2017). Furthermore, by utilizing an application software command-control system, this module may be readily maintained and monitored. Data encryption and decryption are used in processing to safeguard communication. It is not, however, a ready-made device, and this module must be developed individually for the application.

iii. The Actuation Module. This module is in charge of turning on physical equipment and transmitting conditions to IoT entities through the environment. The processed data (also known as the result) will trigger the actuator to execute the result after the raw data has been processed by the processing module. In this module, there is no communication data or computer activity (Chourabi et al., 2012).

iv. The Communication Module. This component is required by all network systems. IoT devices, like any other sort of communication, have an IP address and a location. Because it is a critical module, data or results may be sent from the processing module to the network environment, such as a local area network or a wide area network. Because it links to or from the channel of communication between application software and local devices, the network connection is always in duplex mode (Nik Zulkipli et al., 2017).

v. The Energy Component. The amount of energy available for each IoT component has constrained the energy consumption of IoT devices (Nik Zulkipli et al., 2017). Each action requires a certain amount of energy, since each step from sensing through actuation, transmission, processing, and storage uses energy (Chourabi et al., 2012).

7.4. Mobile Forensics

Mobile device forensics, also known as MF, is a rapidly expanding field that encompasses a range of disciplines and focuses on extracting digital evidence from mobile devices for use in forensic investigations (Fernando, 2021; Zareen & Baig, 2010). In recent years, the majority of studies on mobile device platforms, data acquisition methods, and data extraction techniques have been carried out (Barmpatsalou et al., 2013). Researchers have extensively examined mobile apps to determine where and how private information is accessed. Choi et al. (2019), for example, analysed the database files of three popular Windows IM programs (KakaoTalk, NateOn, and QQ Messenger) to determine how the apps saved and encrypted their data and whether the databases could be decrypted without the mobile user's password.

Digital forensics, especially in the context of cybercrime investigations, has become increasingly dependent on digital evidence as society becomes more digitally advanced and incorporates technologies such as smart cities, smart buildings, and Industry 4.0. Surveillance cameras, IoT devices, and mobile devices are some examples of potential evidence sources in investigations such as drug or sex trafficking investigations (Zhang et al., 2021). Live memory forensics is a computer forensic technique that involves extracting temporary information from Random Access Memory, which remains effective even if the mobile device is turned off.

However, when conducting mobile forensics, it is common practice to examine both the subscriber identification module card and the phone's internal storage (Sharma et al., 2020). However, in another approach van Zandwijk and Boztas (2019) investigated data from the most popular health app on the iPhone 6, iPhone 7, and iPhone 8. They were able to properly determine the user's walking lengths, walking style, and walking speed using this data, giving a digital footprint that might be used as digital evidence. However, there are numerous unanswered questions and challenges in mobile device and app forensics. This is due, at least in part, to the fast development of mobile devices and apps, as well as the proliferation of available mobile devices during the previous decade. In their different literature analyses on mobile devices and app forensics, both Barmpatsalou et al. (2019) and Manral et al. (2020) recognized that data acquisition from mobile devices remained a major operational and research concern.

The challenge highlighted by Servida and Casey (2019) is evident in the utilization of encryption techniques for data-at-rest and data-in-transit, as well as in dealing with newer devices like IoT devices that lack support from existing commercial solutions. Investigating users' encrypted backup data on mobile devices is also deemed critical, as emphasized by Park et al. (2019). In their study, they examined the KoBackup and HiSuite applications, which are associated with Huawei smartphones, to illustrate how forensic investigators can decrypt encrypted backup data and gain access to sensitive user information.

7.5. Social Media Forensics

Social media evidence is now at the forefront of both conventional and cyber-criminal prosecutions. However, this presents digital forensics with distinct legal and technological challenges (Basumatary & Kalita, 2022). Traditional techniques for the extraction and preservation of forensic evidence are inappropriate for social media forensics. Social media evidence is not self-authenticating; thus, further circumstantial and corroboration evidence is required for authenticity. However, the technological challenges are typically a result of the complexity and diversity of information stored on networks, and the legal issues involve the admissibility of evidence and data collection issues (Arshad et al., 2018).

The majority of social media research has focused on the extraction of data artifacts from devices and online social networks. In addition, integrating and correlating social media data to get insights into a crime is a challenge. In a recent study by Tommasel and Godoy (2019), in a single investigation, often hundreds or even thousands of diverse bits of information are forensically acquired for examination since the data is typically utilized to establish a connection between the suspects, the crime, and the victim. The process of correlating the data is often quite complex and might cause investigators or detectives to experience information overload. Furthermore, the information may not make much sense or benefit the investigation until investigators can manage the data into a unified and coherent representation (Nivedha & Sairam, 2015). Therefore, consistent data representation is vital for efficiently eliminating irrelevant data and gaining useful information and insight. Nevertheless, existing methodologies and tools within the domain do not provide these capabilities.

8. TECHNIQUES AND TOOLS USED TO ACQUIRE DIGITAL EVIDENCE

The most frequently used methods and tools for detecting and cracking down on cyber-criminals include digital investigation with forensics approaches that make use of open-source information. There is a variety of resources and techniques within these domains that may be used to collect information about a malicious attacker (Misra & Arumugam, 2022). This data might be used to build a case against the criminals and track them down. Digital forensics experts are frequently called upon to assist in the combatting of cybercrime by collecting and analysing the data that can be used as evidence in court proceedings (Jalali et al., 2019).

Digital forensics is a method used by law enforcement to investigate crimes by integrating digital evidence to determine what happened. Memory/disk analysis and network forensics are some ofthe components used in forensic investigation. By analysing data gathered from computers and networks, the investigation team may be able to pinpoint additional conspirators (Casino et al., 2021). This might help law enforcement to identify and bring these perpetrators to justice before they can commit more acts of violence.

8.1. Data Collection

The process of identifying, acquiring, and securing electronic data for use as evidence in a civil or criminal legal proceeding is known as digital forensic acquisition (Arshad et al., 2019). Although following the formal acquisition procedure and following legal standards is required for utilizing this information as evidence in court, this process is mainly performed by a person with sufficient skills in legal and technical aspects to assure legally sound acquisition (Karie & Karume, 2017). On social media, forensic artifacts are acknowledged as an important source of evidence. As a result, the majority of research efforts are focused on acquiring forensic evidence. The first research on social media forensic extraction focused on device-specific identification and recovery of traces left on devices by social network applications and web browsers. Typically, the requirements for forensic collection from social networks consists of obtaining pertinent data or content from diverse social media platforms, collecting metadata for social media content, and ensuring data integrity throughout the forensic collection process. (Khanafseh et al., 2019).

8.2. Timeline and Data Analysis Techniques

Several studies (Dadvar et al., 2013; Nandhini & Sheeba, 2015) have presented research on crime detection on social media to automate the identification of cybercrime, such as research on crime detection on social media published in several papers, to automate the identification of cybercrime.

Similarly, a keyword-based strategy for detecting cyberbullying has reportedly been presented by Hon and Varathan (2015) for effective detection of cyber-bullies. A similar approach (Chatzakou et al., 2017) proposes natural language processing (NLP) techniques combined with user behavior and their activities to identify hostile and harassing behaviors. According to Dani et al. (2017), sentiment analysis was employed to identify cyberbullying on social media. Similarly, there are just a few approaches to identifying malware and cyberbullying (Arshad et al., 2019; Dadvar et al., 2013; Nandhini & Sheeba, 2015).

These authors present an approach for detecting cyberbullying on Twitter based on keyword searches (Hon & Varathan, 2015). Similarly, some techniques are devoted to tracking illegal activity and criminal tendencies on social networks such as Facebook and Twitter (Alami & Elbeqqali, 2015). The evidence collection and analysis of online social media content is very crucial because multitenancy and virtualized environments create a serious challenge. However, cyber-criminals take this advantage in launching their attacks (Arshad et al., 2019; Kazaure et al., 2019). Although the social media data is sorted in chronological order, manual examination is not viable to uncover this diverse evidence. A typical chronology may include information over many years, including thousands of actions that are irrelevant to the current investigation.

Consequently, it is vital to develop ways for efficiently detecting cyber-criminals and find a suitable approach that can help to easily identify pertinent data, so that sensitive information that can reveal important findings after the investigation can be realized (Park et al., 2018). On the hand, NLP methods and data mining approaches are appropriate for the automated identification of illegal activities and cybersecurity analysis. They are, nevertheless, unsuitable for forensic investigation and legal presentation for two primary reasons. Initially, legal presentation necessitates the explanation of the logical process used to reach the outcomes of the data mining techniques used (Rossy & Ribaux, 2020).

However, it is challenging to explain the sequence of events that led to the evidence acquired during preprocessing and normalization phases of these approaches, since data provenance may likely be lost. Therefore, it is not possible to link the outcome to the source data (Han, 2016). Second, NLP and data mining approaches rely heavily on data processing techniques based on clustering and probability, which enable rapid identification of illegal conduct with high false positive rates. In automated detection systems, false positives are accepted as a necessary evil, yet they are unacceptable in court rulings (Du et al., 2017). Because real-world data is scarce in cybersecurity research, integrating rigorous analytical procedures with passive and active measurement techniques may provide information on a subject's security posture. Protocols, devices, apps, technologies, platforms, users, and threats are also rapidly expanding on the Internet. Meanwhile, in response to the increasing concern for users' and other organizations' privacy in cyberspace, numerous countermeasures to avoid information breaches have been developed (Servida & Casey, 2019). Although these steps are commendable and necessary, they undoubtedly complicate the collection and analysis of empirical cybersecurity data. As a consequence, adopting Internet evaluation is sometimes challenging and demands the development of novel approaches to assure its correctness and completeness (Valjarevic & Venter, 2013).

9. RECENT ADVANCES AND TECHNIQUES USED FOR CYBERCRIME MITIGATION

Cybercrime is a rapidly evolving threat that poses significant risks to organizations and individuals alike. To address this issue, the cybersecurity industry has developed a range of techniques and technologies aimed at mitigating the impact of cyberattacks. In this paper, some of the recent advances in cybercrime mitigation techniques and their potential to enhance cybersecurity were examined. One significant development in recent years has been the use of artificial intelligence (AI) and ML in cybersecurity. These technologies enable security professionals to detect potential threats and respond to them quickly by identifying patterns of behavior and anomalies in network traffic (Yeboah-Ofori & Brimicombe, 2018).

The advancements in AI and ML contribute to enhancing the precision and efficiency of cybercrime detection through continuous learning from data and adapting to emerging threats. Additionally, the adoption of cloud-based security solutions has become a significant trend. These solutions enable organizations to securely store and process data in the cloud, benefiting from the inherent security features they provide. Cloud-based security offers greater flexibility and scalability compared to traditional on-premises solutions, empowering organizations to monitor and safeguard their systems from any location. Another noteworthy development in combating cybercrime is the utilization of blockchain technology, as highlighted by Ficco et al. (2015). The distributed ledger technology has the potential to create a more secure and decentralized Internet, making it more difficult for cybercriminals to carry out attacks. However, blockchain can be used to secure transactions and prevent fraud, making it an attractive technology for organizations looking to enhance their cybersecurity architecture (Rathee, 2020). Multifactor authentication is another technique that has gained prominence in recent years. This technology requires users to provide two or more forms of authentication before accessing a system.

This additional layer of security helps prevent unauthorized access to sensitive data and systems, making it an effective way to mitigate the risks of cybercrime. In addition to these techniques, several other recent advances in cybercrime mitigation are worth noting. Threat intelligence involves collecting and analysing data from various sources to identify and prevent cyber threats. Zero trust security assumes that all users, devices, and network traffic are potentially hostile, requiring strict identity verification and access controls for all users. Next-generation firewalls combine traditional firewall technology with advanced security features to provide enhanced security capabilities. Endpoint detection and response detects and responds to threats on endpoints such as laptops, desktops, and mobile devices. Finally, security orchestration, automation, and response automates the response to security events, integrating with various security tools to detect and respond to threats automatically.

10. CYBERCRIME MITIGATION TECHNIQUES

The proliferation of cybercrime has outpaced the ability of traditional forensics-based detection systems to fully prevent or mitigate such attacks. This is largely due to the diverse range of targets (e.g. individuals, banks, businesses, and governments) and motivations (e.g. financial gain, notoriety, sexual exploitation, curiosity) behind cybercrimes, coupled with the constant evolution and adoption of new technologies by cyber-criminals (Yeboah-Ofori & Brimicombe, 2018). Cybercrimes refer to criminal acts, ranging from minor offenses to serious indictable crimes, that are perpetrated through or against computer systems and communication devices (Arfaj et al., 2022). Common examples of cybercrimes include, but are not limited to, cyberstalking, identity theft, credit card fraud, child pornography, cyber laundering, drug sales, cyber terrorism, data breaches, phishing, sexually explicit content, and various types of cyber hacking (Al-Khater et al., 2020). Such offenses often result in breaches of privacy, security violations, financial fraud, business losses, or damage to public or government properties. However, previous studies have been conducted with the objective of devising efficient approaches to detecting cybercrimes. These methods are commonly categorized into various groups, as presented in Fig. 5 and expounded upon in the following sections.

10.1. Machine Learning Techniques

Cybercrime detection using ML techniques has gained significant attention in recent years (Sharma et al., 2021). ML algorithms can be used to analyse large amounts of data and identify patterns, anomalies, and potential threats in various cyber activities. ML incorporates the process of making predictions based on input data, commonly known as training data (Sandoval-Orozco et al., 2020). Through this process, computers acquire the ability to accurately predict suitable outputs for specific inputs using the provided training data.

The learning process can be categorized as either supervised or unsupervised. In supervised learning, the training data consists of input-output pairs, with the outputs referred to as labeled outputs due to their predetermined correctness. In a study conducted by Fortuna and Nunes (2018), they utilized three supervised ML methods (JRip, J48, and Support Vector Machine) to detect instances of cyberbullying in YouTube comments. They also compared a binary classifier and a multi-classifier. Conversely, Al-garadi et al. (2016) proposed a tool for identifying cyberbullying in tweets, where they extracted various features from each tweet to be used in the classifier. They experimented with different classifiers, including support vector machines, naive Bayes, K nearest neighbor, and decision trees, to determine the most effective one.

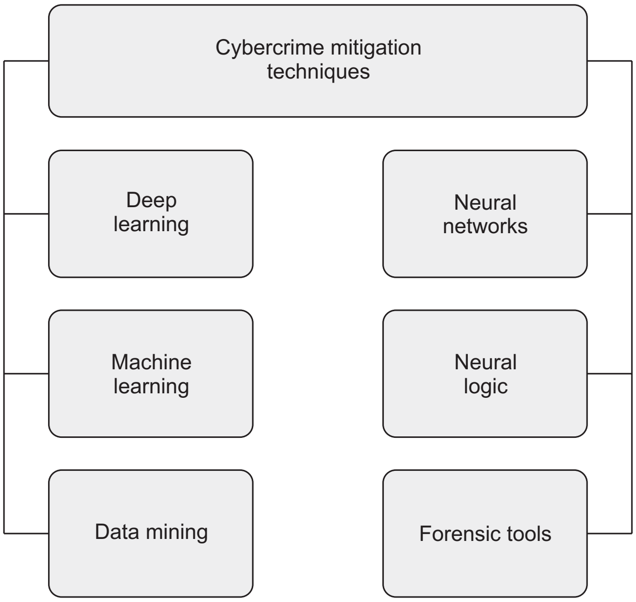

Fig. 5. Cybercrime mitigation techniques.

The authors concluded that naive Bayes demonstrated superior performance and sufficient strength, based on the findings of Al-garadi et al. (2016). In a similar approach, Uzel et al. (2018) employed text classification to recognize cyber terror and extremism (CTE). Their method involved assigning numerical weights to terms to identify CTE-related vocabulary within texts, followed by converting the document into a vector representation.

10.1.1. Data Mining

Data mining techniques are widely used in the detection of cybercrime (Tommasel & Godoy, 2019). These techniques leverage large volumes of data to identify patterns, anomalies, and relationships that help in uncovering and mitigating cyber threats. Some common data mining approaches in cybercrime detection include anomaly detection, classification, clustering, association rule mining, text mining, and network traffic analysis (Mohammad, 2020). By employing these techniques, organizations can enhance their ability to detect and respond to cyber threats, leading to improved security and protection against cyber-criminal activities (Ukwen & Karabatak, 2021).

10.1.2. Neural Networks

Neural networks, including feedforward neural networks, recurrent neural networks, convolutional neural networks, deep belief networks, and long short-term memory networks, are commonly used in detecting cybercrime (Subba et al., 2018). These techniques enable the processing of complex patterns and temporal dependencies in data, allowing for the identification of known and emerging cyber threats. By leveraging the capabilities of neural networks, organizations can enhance their cybercrime detection systems and improve their ability to combat cyber-criminal activities (Karami, 2018).

10.1.3. Neural Logic

Neural logic techniques can be employed for cybercrime detection by combining neural networks and logical reasoning, resulting in improved accuracy and effectiveness of detection systems (Al-Khater et al., 2020). Here are some ways in which neural logic techniques can be applied:

a) Rule-based learning: Neural networks can be trained to learn rules or logical patterns from labeled data. By integrating logical constraints or rules into the neural network architecture, it becomes possible to capture complex patterns in cybercrime data and incorporate explicit knowledge represented by logical rules. This hybrid approach enables the detection of cybercrime activities based on learned patterns that align with logical rules.

b) Explainable AI: Neural logic techniques enhance the interpretability and explainability of cybercrime detection models. By integrating logical rules or constraints into neural networks, the system can provide human-understandable explanations for its decisions. This helps cybersecurity experts comprehend why certain instances are classified as cybercrime, fostering trust and transparency in the detection process.

c) Fuzzy logic integration: Fuzzy logic, capable of handling uncertainty and imprecise data, can be combined with neural networks to enhance cybercrime detection. Fuzzy logic enables the representation of uncertain or vague rules, which can be integrated with neural networks to handle complex and uncertain cybercrime scenarios.

d) Neuro-symbolic approaches: Neuro-symbolic AI combines neural networks with symbolic reasoning techniques, such as logical inference or knowledge graphs. This integration exploits the statistical learning capabilities of neural networks and the logical reasoning abilities of symbolic systems. By encoding cybercrime-related knowledge into a knowledge graph and training neural networks based on it, the system can leverage the strengths of both paradigms, leading to more accurate cybercrime detection.

However, by incorporating neural logic techniques, cybercrime detection systems can benefit from the combination of neural networks' learning abilities and logical reasoning's rule-based approach, resulting in enhanced detection accuracy, interpretability, and transparency.

10.1.4. Use of Forensic Tools

The use of forensic tools is critical in mitigating cybercrimes. Forensic tools can aid in the collection, analysis, and preservation of digital evidence, which is essential in identifying and prosecuting cyber-criminals (Stoykova et al., 2022). Forensic tools such as digital imaging software can make an exact copy of the data on a device, ensuring that the original data is not altered or destroyed during the investigation process (Servida & Casey, 2019). Data recovery software can also be used to retrieve deleted or lost data that may contain critical evidence. Additionally, forensic tools such as network analysis software can be used to examine network traffic and identify patterns of suspicious behavior (Wu et al., 2020). This can aid in identifying cyberattacks such as DoS attacks, phishing attempts, or malware infections. Furthermore, forensic tools can be used to investigate cybercrimes such as identity theft, cyberstalking, and cyberbullying. Digital forensics techniques can reveal valuable information about the suspect's activities, including their online communications, online transactions, and browsing history (Javed et al., 2022).

11. APPROACHES SO FAR IN MITIGATING CYBERCRIMES

In terms of communication, relationships, and particularly interconnection, the world is growing smaller and smaller every day. The IoT is on the increase, since everything is increasingly linked via the available networks. Various businesses are collaborating to develop sector-spanning interconnections. Because so many people utilize the Internet daily, they lack awareness of the significance of cybersecurity (de Bruijnm & Janssen, 2017). The majority of users only create accounts as required, notably inside their apps, even though they are not designed as robustly as possible. The transmission of information enables the existence of physical infrastructure in cyberspace. If one is unaware of the significance of cybersecurity software, one will not secure devices and systems adequately. Today, we save all of our data on the cloud, so if someone has access to the cloud, they may harm a person technologically (Agrafiotis et al., 2018). These occurrences result in identity theft and monetary losses, among other damages. It is necessary to raise public understanding of the significance of cybersecurity for the populace to comprehend its need. IT department employees have the benefit of recognizing the hazards of cyberattacks and taking the necessary precautions. Even though it is not sufficient inside an organization, malicious hackers will check out and attack the weakest link (Tian et al., 2020).

According to de Bruijnm and Janssen (2017), so many people believe that the cyber-physical society will resolve all issues on its own. They forget that the harm that may be caused might also affect them directly. This ignorance must be erased by educating people on the significance of cybersecurity and the most effective means of achieving it in our society. Cybersecurity is an ongoing issue that needs serious attention from both the government and individuals so that when addressing the problems things will not fall apart. In light of this, cyber threats must be observed in all aspects of our interactions in cyberspace (Maalem Lahcen et al., 2020). To be effective, cybersecurity applications must pay attention to good use of existing cybersecurity knowledge to develop countermeasures against cyberattacks.

However, to tackle these problems the similar attacks that have been mounted must be taken into consideration. The strategies used here will attempt to seal any holes that could have been present in earlier attempts. This is an example of the more common "prevention by elimination" strategy. The things that are already known or thought about should be included as a foundation for cybersecurity. Secondly, new weaknesses in cybersecurity must be constantly reported, meaning getting ready for something that is not manifested and not known. Experts need to be ready for both the known and the unknown threats that may arise anytime (Yaacoub et al., 2022).

12. ANALYSIS OF FINDINGS BASED ON THE REVIEW

Forensic professionals play a crucial role in mitigating cybercrimes by collecting and analysing digital evidence from computer systems and mobile devices. The following are some of the techniques and methods used by forensic professionals in mitigating cybercrimes:

a) Data collection: Forensic professionals collect digital evidence from various sources, including computer systems, mobile devices, and cloud storage. They use specialized tools and techniques to ensure that the data is collected in a forensically sound manner, without altering or damaging the original evidence.

b) Data analysis: Once the data has been collected, forensic professionals use various analytical tools and methods to analyse the evidence. This includes examining file headers, metadata, and other artifacts to determine the source, nature, and extent of the cybercrime.

c) Data recovery: In some cases, digital evidence may be deleted, encrypted, or damaged. Forensic professionals use specialized tools and techniques to recover such data, which may be crucial in establishing the cause and extent of the cybercrime.

d) Data preservation: It is essential to preserve the integrity of the digital evidence throughout the investigation. Forensic professionals use techniques such as write-blocking, hashing, and chain of custody documentation to ensure that the data is not tampered with, changed, or destroyed.

e) Data provenance: Data provenance refers to the record of the sources, usage, update, and processing of data. Forensic professionals use this technique to trace the sources and causes of any cyberspace-based issues.

f) Malware analysis: Malware is a common tool used by cyber-criminals to gain unauthorized access to computer systems and networks. Forensic professionals use specialized tools and techniques to analyse malware, which can provide valuable insights into the nature and extent of cybercrime.

g) Network analysis: Cyber-criminals often use networks to carry out their attacks. Forensic professionals use network analysis techniques to trace the source of the attack, identify compromised systems, and determine the extent of the damage.

However, forensic professionals play a critical role in mitigating cybercrimes by collecting and analysing digital evidence from computer systems and mobile devices. They use a variety of specialized tools and techniques to ensure that the data is collected in a forensically sound manner and that the integrity of the evidence is preserved throughout the investigation. By using these techniques and methods, forensic professionals can help to identify cyber-criminals, prosecute them, and reduce the incidence of cybercrime.

13. CONCLUSION

In conclusion, cybercrime is a significant threat to individuals and organizations, and it is essential to have effective measures in place to mitigate its impact. Forensic professionals play a critical role in investigating cybercrime and collecting legally acceptable evidence using modern techniques to handle a large amount of computer and other digital media information. Techniques such as data provenance, malware analysis, memory forensics, and network forensics are valuable tools for forensic investigators in mitigating cybercrime.

However, to be successful in investigating cybercrime, forensic professionals must follow a legally and scientifically appropriate forensic process that respects people's privacy rights. They must ensure that no evidence is tampered with, changed, or destroyed throughout the operation. Additionally, they must keep up with the most current cybercrime issues and mitigating procedures, including new forensic techniques and software. Lastly, as the number of cyber threats continues to grow, forensic professionals must remain vigilant and work together with other cybersecurity professionals to stay one step ahead of cyber-criminals. By utilizing the latest techniques and methods, they can help mitigate the impact of cybercrime and protect individuals and organizations from its damaging effects.

ACKNOWLEDGEMENTS

The authors of this study express their gratitude towards the Security & Forensic Research Group (SFRG) Laboratory, School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia, for their assistance in procuring the necessary materials for the research work. The support and cooperation of the laboratory staff and students were essential in ensuring the success of the study. Additionally, the authors extend their appreciation to the reviewers who provided valuable feedback and recommendations that helped improve the quality of the research. The reviewers' insights and suggestions have been instrumental in enhancing the presentation of this research endeavor. Without the contribution of the SFRG Laboratory and the reviewers, this study would not have been possible. The authors are grateful for their assistance and acknowledge their contribution to the success of this research work.

CONFLICTS OF INTEREST

No potential conflict of interest relevant to this article was reported.

REFERENCES

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Akbari, Y., Al-maadeed, S., Elharrouss, O., Khelifi, F., Lawgaly, A., & Bouridane, A. (2022). Digital forensic analysis for source video identification: A survey. *Forensic Science International: Digital Investigation,* 41, 301390. https://doi.org/10.1016/j.fsidi.2022.301390

Al-Dhaqm, A., Razak, S., Othman, S. H., Choo, K. K. R., Glisson, W. B., Ali, A., & Abrar, M. (2017). CDBFIP: Common database forensic investigation processes for internet of things. *IEEE Access,* 5, 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

Al-garadi, M. A., Varathan, K. D., & Ravana, S. D. (2016). Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior,* 63, 433-443. https://

doi.org/10.1016/j.chb.2016.05.051

Al-Khateeb, S., Hussain, M. N., & Agarwal, N. (2019). Leveraging social network analysis and cyber forensics approaches to study cyber propaganda campaigns. In T. Özyer, S. Bakshi, & R. Alhajj (Eds.), *Social networks and surveillance for society* (pp. 19-42). Springer.

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access,* 8, 137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

Alami, S., & Elbeqqali, O. (2015, October 20-21). Cybercrime profiling: Text mining techniques to detect and predict criminal activities in microblog posts. *Proceedings of the 10th International Conference on Intelligent Systems: Theories and Applications (SITA)* (pp. 1-5). IEEE.

Arfaj, B. A. B., Mishra, S., & Alshehri, M. (2022). Efficacy of unconventional penetration testing practices. *Intelligent Automation & Soft Computing,* 31(1), 223-239. https://doi.org/10.32604/iasc.2022.019485

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers & Security,* 105, 102237. https://doi.org/10.1016/j.cose.2021.102237

Arshad, H., Jantan, A., & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems,* 14(2), 346-376. https://doi.org/10.3745/JIPS.03.0095

Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation,* 28, 126-138. https://doi.org/10.1016/j.diin.2019.02.001

Awasthi, A., Read, H. O. L., Xynos, K., & Sutherland, I. (2018). Welcome pwn: Almond smart home hub forensics. *Digital Investigation,* 26, S38-S46. https://doi.org/10.1016/j.diin.2018.04.014

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation,* 22, 3-13. https://doi.org/10.1016/j.diin.2017.06.015

Bankole, F. O., Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation,* 40, 301348. https://doi.org/10.1016/j.fsidi.2022.301348

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2019). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys,* 51(3), 46. https://doi.org/10.1145/3177847

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of mobile device forensics. *Digital Investigation,* 10(4), 323-349. https://doi.org/10.1016/j.diin.2013.10.003

Basumatary, B., & Kalita, H. K. (2022, March 23-25). Social media forensics - A holistic review. In D. Saini (Ed.), *Proceedings of the 9th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 590-597). IEEE.

Bennett, J. C., & Diallo, M. H. (2018, October 24-26). A forensic pattern-based approach for investigations in cloud system environments. *Proceedings of the 2nd Cyber Security in Networking Conference (CSNet)* (pp. 1-8). IEEE.

Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2017). *Equifax says cyberattack may have affected 143 million in the U.S. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html*

Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse & Neglect,* 44, 140-149. https://doi.org/10.1016/j.chiabu.2014.12.004

Carrier, B. D., & Spafford, E. H. (2004, August 11-13). An event-based digital forensic investigation framework. *Proceedings of the 2004 Digital Forensic Research Conference* (pp. 1-12). DFRWS.

Casey, E., & Souvignet, T. R. (2020). Digital transformation risk management in forensic science laboratories. *Forensic Science International,* 316, 110486. https://doi.org/10.1016/j.forsciint.2020.110486

Casino, F., Dasaklis, T., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2021). Research trends, challenges, and emerging topics of digital forensics: A review of reviews. *arXiv.* https://doi.org/10.48550/arXiv.2108.04634

Chatzakou, D., Kourtellis, N., Blackburn, J., De Cristofaro, E., Stringhini, G., & Vakali, A. (2017, June 25-28). Mean birds: Detecting aggression and bullying on Twitter. *Proceedings of the 2017 ACM Web Science Conference (WebSci '17)* (pp. 13-22). ACM.

Choi, J., Yu, J., Hyun, S., & Kim, H. (2019). Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger. *Digital Investigation,* 28, S50-S59. https://doi.org/10.1016/j.diin.2019.01.011

Choo, K. K. R., & Dehghantanha, A. (2017). Contemporary digital forensics investigations of cloud and mobile applications. In K. K. R. Choo, & A. Dehghantanha (Eds.), *Contemporary digital forensic investigations of cloud and mobile applications* (pp. 1-6). Syngress.

Choo, K. K. R., Esposito, C., & Castiglione, A. (2017). Evidence and forensics in the cloud: Challenges and future research directions. *IEEE Cloud Computing,* 4(3), 14-19. https://doi.org/10.1109/MCC.2017.39

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012, January 4-7). Understanding smart cities: An integrative framework. In R. H. Jr. Sprague (Ed.), *Proceedings of the 45th Hawaii International Conference on System Sciences* (pp. 2289-2297). IEEE.

Chuprat, S., Ariffin, A., Sahibuddin, S., Mahrin, M. N., Senan, F. M., Ahmad, N. A., Narayana, G., Magalingam, P., Anuar, S., & Talib, M. Z. (2018, November 15-16). Malware forensic analytics framework using big data platform. In K. Arai, R. Bhatia, & S. Kapoor (Eds.), *Proceedings of the Future Technologies Conference 2018 (FTC 2018)* (pp. 261-274). Springer.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence,* 3(1), 1-22. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93C-C575FA.pdf

Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity,* 6(1), tyaa023. https://doi.org/10.1093/cybsec/tyaa023

Dadvar, M., Trieschnigg, D., Ordelman, R., & de Jong, F. (2013, March 24-27). Improving cyberbullying detection with user context. In P. Serdyukov, P. Braslavski, S. O. Kuznetsov, J. Kamps, S. Rüger, E. Agichtein, I. Segalovich, & E. Yilmaz (Eds.), *Proceedings of the 35th European Conference on IR Research* (pp. 693-696). Springer.

Dani, H., Li, J., & Liu, H. (2017, September 18-22). Sentiment informed cyberbullying detection in social media. In M. Ceci, J. Hollmén, L. Todorovski, C. Vens, & S. Džeroski (Eds.), *Proceedings of the 2017 European Conference on Machine Learning and Knowledge Discovery in Databases* (pp. 52-67). Springer.

de Bruijnm H., & Janssen, M. F. W. H. A. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly,* 34(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array,* 5, 100015. https://doi.org/10.1016/j.array.2019.100015

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *arXiv.* https://doi.org/10.48550/arXiv.1708.01730

Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation,* 10, S87-S95. https://doi.org/10.1016/j.diin.2013.06.010

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology,* 49(1), 45-55. https://doi.org/10.1111/bjet.12529

Fernando, V. (2021, April 19-21). Cyber forensics tools: A review on mechanism and emerging challenges. *Proceedings of the 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-7). IEEE.

Ficco, M., Palmieri, F., & Castiglione, A. (2015). Modeling security requirements for cloud-based system development. *Concurrency and Computation: Practice and Experience,* 27(8), 2107-2124. https://doi.org/10.1002/cpe.3402

Flores, R., Siami Namin, A., Tavakoli, N., Siami-Namini, S., & Jones, K. S. (2021). Using experiential learning to teach and learn digital forensics: Educator and student perspectives. *Computers and Education Open,* 2, 100045. https://doi.org/10.1016/j.caeo.2021.100045

Fortuna, P., & Nunes, S. (2018). A survey on automatic detection of hate speech in text. *ACM Computing Surveys,* 51(4), 85. https://doi.org/10.1145/3232676

Freiling, F. C., & Schwittay, B. (2007, September 11-13). A common process model for incident response and computer forensics. In O. Göbel, D. Günther, H. G. Hase, J. Nedon, D. Schadt, A. Brömme, & S. Frings (Eds.), *Proceedings of the 3rd International Conference on IT-Incident Management + IT-Forensics* (pp. 19-39). Gesellschaft für Informatik.

Grover, R., Krishna, C. R., Mishra, A. K., Pilli, E. S., & Govil, M. C. (2016, October 19-21). A comparison of analysis approaches for cloud forensics. *Proceedings of the 2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)* (pp. 131-135). IEEE.

Guo, Z., Cho, J. H., Chen, I. R., Sengupta, S., Hong, M., & Mitra, T. (2021). Online social deception and its countermeasures: A survey. *IEEE Access,* 9, 1770-1806. https://doi.org/10.1109/ACCESS.2020.3047337

Han, F. (2016). Cloud based forensics framework for social networks and a case study on reasoning links between nodes. *International Journal of Future Generation Communication and Networking,* 9(1), 23-34. https://doi.org/10.14257/ijfgcn.2016.9.1.03

Hargreaves, C., & Patterson, J. (2012). An automated timeline reconstruction approach for digital forensic investigations. *Digital Investigation,* 9, S69-S79. https://doi.org/10.1016/j.diin.2012.05.006

Hemdan, E. E. D., & Manjaiah, D. (2021). An efficient digital forensic model for cybercrimes investigation in cloud computing. *Multimedia Tools and Applications,* 80(9), 14255-14282. https://doi.org/10.1007/s11042-020-10358-x

Hill, S., & Swinhoe, D. (2022). *The 15 biggest data breaches of the 21st century.* https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* Routledge.

Hon, L. C., & Varathan, K. D. (2015). Cyberbullying detection on Twitter. *International Journal of Information System and Engineering*, 3(1), 36-47.

Horan, C., & Saiedian, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy,* 1(4), 580-596. https://doi.org/10.3390/jcp1040029

Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers & Security,* 73, 294-306. https://doi.org/10.1016/j.cose.2017.11.009

Horsman, G. (2020). Part 1: Quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework. *Forensic Science International: Reports,* 2, 100038. https://doi.org/10.1016/j.fsir.2019.100038

Horsman, G. (2022). The Hierarchy of Case Priority (HiCaP): A proposed method for case prioritisation in digital forensic laboratories. *Science & Justice,* 62(5), 594-601. https://doi.org/10.1016/j.scijus.2022.08.008

Internet Crime Complaint Center (IC3). (2020). *2020 Internet crime report.* IC3.

Interpol. (2020). *Interpol report highlights impact of COVID-19 on child sexual abuse.* https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems,* 28(1), 66-82. https://doi.org/10.1016/j.jsis.2018.09.003

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access,* 10, 11065-11089. https://doi.org/10.1109/ACCESS.2022.3142508

Karami, A. (2018). An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications,* 108, 36-60. https://doi.org/10.1016/j.eswa.2018.04.038

Karie, N. M., & Karume, S. M. (2017). Digital forensic readiness in organizations: Issues and challenges. *Journal of Digital Forensics, Security and Law,* 12, Article 5. https://doi.org/10.15394/jdfsl.2017.1436

Karie, N. M., Kebande, V. R., & Venter, H. S. (2016, July 7-8). A generic framework for digital evidence traceability. *Proceedings of the 15th European Conference on Cyber Warfare and Security (ECCWS)* (pp. 361-369). ECCWS.

Kazaure, A. A., Jantan, A., Yusoff, M. N., Maigari, A., Ishak, M. K., & Noor, N. R. M. (2019). Evidence collection and forensic challenges in cloud environment. *MACE Technical Journal,* 1(1), 8-18.

Kebande, V. R., & Ray, I. (2016, August 22-24). A generic digital forensic investigation framework for internet of things (IoT). In M. Younas & W. Seah (Eds.), *Proceedings of the 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 356-362). IEEE.

Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K. K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Science International: Reports,* 2, 100117. https://doi.org/10.1016/j.fsir.2020.100117

Khanafseh, M., Qatawneh, M., & Almobaideen, W. (2019). A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. *International Journal of Advanced Computer Science and Applications,* 10(8), 610-629. https://doi.org/10.14569/IJACSA.2019.0100880

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security,* 38, 103-115. https://doi.org/10.1016/j.cose.2013.05.001

Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017, April 2-6). PayBreak: Defense against cryptographic ransomware. In F. Aloul & M. Maniatakos (Eds.), *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 599-611). ACM.

Kumar Raju, B. K. S. P., Moharil, B., & Geethakumari, G. (2016, December 6-9). FaaSeC: Enabling forensics-as-a-service for cloud computing systems. *Proceedings of the IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC).* (pp. 220-227). IEEE.

Lee H. C., Palmbach, T., & Miller, M. T. (2001). *Henry Lee's crime scene handbook.* Academic Press.

Lewis, R., Rowe, M., & Wiper, C. (2017). Online abuse of feminists as an emerging form of violence against women and girls. *British Journal of Criminology,* 57(6), 1462-1481. https://doi.org/10.1093/bjc/azw073

Lutui, R. (2016). A multidisciplinary digital forensic investigation process model. *Business Horizons,* 59(6), 593-604. https://doi.org/10.1016/j.bushor.2016.08.001

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecur,* 3, 10. https://doi.org/10.1186/s42400-020-00050-w

Manral, B., Somani, G., Choo, K. K. R., Conti, M., & Gaur, M. S. (2020). A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Computing Surveys,* 52(6), 1-38. https://doi.org/10.1145/3361216

Marshall, A. M. (2021). Digital forensic tool verification: An evaluation of options for establishing trustworthiness. *Forensic Science International: Digital Investigation,* 38, 301181. https://doi.org/10.1016/j.fsidi.2021.301181

McCullough, S., Abudu, S., Onwubuariri, E., & Baggili, I. (2021). Another brick in the wall: An exploratory analysis of digital forensics programs in the United States. *Forensic Science International: Digital Investigation,* 37, 301187. https://doi.org/10.1016/j.fsidi.2021.301187

Misra, S., & Arumugam, C. (2022). *Illumination of artificial intelligence in cybersecurity and forensics*. Springer.

Mohammad, R. M. A. (2020). An improved multi-class classification algorithm based on association classification approach and its application to spam emails. *IAENG International Journal of Computer Science,* 47(2), IJCS_47_2_07. https://www.iaeng.org/IJCS/issues_v47/issue_2/IJCS_47_2_07.pdf

Mohammad, R. M. A., & Alqahtani, M. (2019). A comparison of machine learning techniques for file system forensics analysis. *Journal of Information Security and Applications,* 46, 53-61. https://doi.org/10.1016/j.jisa.2019.02.009

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports,* 23(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Morgan, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025. Special report: Cyberwarfare in the C-suite.* https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Moussaileb, R., Bouget, B., Palisse, A., Le Bouder, H., Cuppens, N., & Lanet, J. L. (2018, August 27-30). Ransomware's early mitigation mechanisms. *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. Article No. 2). ACM.

Nandhini, B. S., & Sheeba, J. I. (2015). Online social network bullying detection using intelligence techniques. *Procedia Computer Science,* 45, 485-492. https://doi.org/10.1016/j.procs.2015.03.085

National Institute of Standards and Technology. (2019). *Computer forensics tools & techniques catalog.* https://toolcatalog.nist.gov/

Nik Zulkipli, N. H., Alenezi, A., & Wills, G. B. (2017, April 24-26). IoT forensic: Bridging the challenges in digital forensic and the Internet of Things. In M. Ramachandran, V. M. Muñoz, V. Kantere, G. Wills, R. Walters, & V. Chang (Eds.), *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security IoTBDS* (pp. 315-324). SciTePress.

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation,* 33, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

Nisioti, A., Loukas, G., Mylonas, A., & Panaousis, E. (2023). Forensics for multi-stage cyber incidents: Survey and future directions. *Forensic Science International: Digital Investigation,* 44, 301480. https://doi.org/10.1016/j.fsidi.2022.301480

Nivedha, R., & Sairam, N. (2015). A machine learning based classification for social media messages. *Indian Journal of Science and Technology,* 8(16), 1-4. https://doi.org/10.17485/ijst/2015/v8i16/63640

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013, October 20-23). Internet of Things forensics: Challenges and approaches. In E. Bertino, D. Georgakopoulos, M. Srivatsa, S. Nepal, & A. Vinciarelli (Eds.), *Proceedings of the 1st International Workshop on Internet of Things.* ICST.

Park, M., Kim, G., Park, Y., Lee, I., & Kim, J. (2019). Decrypting password-based encrypted backup data for Huawei smartphones. *Digital Investigation,* 28, 119-125. https://doi.org/10.1016/j.diin.2019.01.008

Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., Shin, H, Han, C., & Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digital Investigation,* 24 Suppl, S93-S100. https://doi.org/10.1016/j.diin.2018.01.012

Pitchkites, M. (2022). *Top cyber security statistics, facts & trends in 2023.* https://www.cloudwards.net/cyber-security-statistics/

Pour, M. S., Nader, C., Friday, K., & Bou-Harb, E. (2023). A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security,* 128, 103123. https://doi.org/10.1016/j.cose.2023.103123

Ptaszynski, M., Eronen, J. K. K., & Masui, F. (2017, August 21). Learning deep on cyberbullying is always better than brute force. In R. Rzepka, J. Vallverdu, & A. Wlodarczyk (Eds.), *Proceedings of the Linguistic and Cognitive Approaches to Dialog Agents Workshop co-located with the 26th International Joint Conference on Artificial Intelligence* (pp. 3-10). CEUR-WS.

Rathee, P. (2020). Introduction to blockchain and IoT. In S. Kim, & G. Deka (Eds.), *Advanced applications of blockchain technology: Vol. 60. Studies in big data* (pp. 1-14). Springer.

Rossy, Q., & Ribaux, O. (2020). Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. *European Journal on Criminal Policy and Research,* 26(3), 335-356. https://doi.org/10.1007/s10610-020-09438-3

Sandoval-Orozco, A. L., Quinto Huamán, C., Povedano Álvarez, D., & García Villalba, L. J. (2020). A machine learning forensics technique to detect post-processing in digital videos. *Future Generation Computer Systems,* 111, 199-212. https://doi.org/10.1016/j.future.2020.04.041

Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation,* 28 Suppl, S22-S29. https://doi.org/10.1016/j.diin.2019.01.012

Sharma, P., Arora, D., & Sakthivel, T. (2020). Enhanced forensic process for improving mobile cloud traceability in cloud-based mobile applications. *Procedia Computer Science,* 167, 907-917. https://doi.org/10.1016/j.procs.2020.03.390

Sharma, S., Krishna, C. R., & Kumar, R. (2021). RansomDroid: Forensic analysis and detection of Android Ransomware using unsupervised machine learning technique. *Forensic Science International: Digital Investigation,* 37, 301168. https://doi.org/10.1016/j.fsidi.2021.301168

Spruit, M., & Röling, M. (2014). *ISFAM: The information security focus area maturity model*. Paper presented at the 22nd European Conference on Information Systems, Tel Aviv, Israel.

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation,* 40, 301351. https://doi.org/10.1016/j.fsidi.2022.301351

Subba, B., Biswas, S., & Karmakar, S. (2018). A game theory based multi layered intrusion detection framework for VANET. *Future Generation Computer Systems,* 82, 12-28. https://doi.org/10.1016/j.future.2017.12.008

Sultan, N. (2021). Cybersecurity incident response: Incident handling and response approaches. In M. M. Cruz-Cunha, & I. M. Portela (Eds.), *Handbook of research on digital crime, cyberspace security, and information assurance* (pp. 233-246). IGI Global.

Sun, D., Zhang, X., Choo, K. K. R., Hu, L., & Wang, F. (2021). NLP-based digital forensic investigation platform for online communications. *Computers & Security,* 104, 102210. https://doi.org/10.1016/j.cose.2021.102210

Sunde, N., & Horsman, G. (2021). Part 2: The phase-oriented advice and review structure (PARS) for digital forensic investigations. *Forensic Science International: Digital Investigation,* 36, 301074. https://doi.org/10.1016/j.fsidi.2020.301074

The White House. (2021). *Statement by Press Secretary Jen Psaki on the executive order on improving the nation's cybersecurity.* https://www.whitehouse.gov/briefing-room/statementsreleases/2021/04/15/statement-by-press-secretary-jen-psaki-on-the-executive-order-on-improving-the-nations-cybersecurity

Tian, J., Bi, Y., & Ma, J. (2020). Research on forensics of social network relationship based on big data. *Journal of Physics: Conference Series,* 1584, 012022. https://doi.org/10.1088/1742-6596/1584/1/012022

Tommasel, A., & Godoy, D. (2019). Short-text learning in social media: A review. *Knowledge Engineering Review,* 34, e7. https://doi.org/10.1017/S0269888919000018

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers & Security,* 83, 22-37. https://doi.org/10.1016/j.cose.2019.01.011

Turnbull, B., & Randhawa, S. (2015). Automated event and social network extraction from digital evidence sources with ontological mapping. *Digital Investigation,* 13, 94-106. https://doi.org/10.1016/j.diin.2015.04.004

Tymoshenko, Y. P., Kozachenko, O. I., Kyslenko, D. P., Horodetska, M. S., Chubata, M. V., & Barhan, S. S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga,* 11(51), 149-160. https://doi.org/10.34069/AI/2022.51.03.14

Ukwen, D. O., & Karabatak, M. (2021, June 28-29). Review of NLP-based systems in digital forensics and cybersecurity. In A. Varol, M. Karabatak, & C. Varol (Eds.), *Proceedings of the 9th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-9). IEEE.

Uzel, V. N., Saraç Eşsiz, E., & Ayşe Özel, S. (2018, October 4-6). Using fuzzy sets for detecting cyber terrorism and extremism in the text. In B. M. Ozyildirim, & T. Yildirim (Eds.), *Proceedings of the 2018 Innovations in Intelligent Systems and Applications Conference (ASYU)* (pp. 1-4). IEEE.

Valjarevic, A., & Venter, H. (2013, January 28-30). A harmonized process model for digital forensic investigation readiness. In G. Peterson, & S. Shenoi (Eds.), *Proceedings of the 9th IFIP WG 11.9 International Conference on Digital*

Forensics (pp. 67-82). Springer.

van Zandwijk, J. P., & Boztas, A. (2019). The iPhone health app from a forensic perspective: Can steps and distances registered during walking and running be used as digital evidence? *Digital Investigation,* 28 Suppl, S126-S133. https://doi.org/10.1016/j.diin.2019.01.021

Weiss, N. E., & Miller, R. S. (2015). *The target and other financial data breaches: Frequently asked questions.* Congressional Research Service.

Wu, T., Breitinger, F., & O'Shaughnessy, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation,* 34, 300999. https://doi.org/10.1016/j.fsidi.2020.300999

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security,* 21(1), 115-158. https://doi.org/10.1007/s10207-021-00545-8

Yeboah-Ofori, A., & Brimicombe, A. (2018). Cyber intelligence and OSINT: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics,* 7(1), 87-98. https://doi.org/10.17781/p002378

Zareen, A., & Baig, S. (2010, May 20). Notice of violation of IEEE publication principles: Mobile phone forensics: Challenges, analysis and tools classification. *Proceedings of the 5th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 47-55). IEEE.

Zawoad, S., & Hasan, R. (2015, June 27-July 2). FAIoT: Towards building a forensics aware eco system for the internet of things. In P. P. Maglio, I. Paik, & W. Chou (Eds.), *Proceedings of the 2015 IEEE International Conference on Services Computing* (pp. 279-284). IEEE.

Zhang, X., Liu, C. Z., Choo, K. K. R., & Alvarado, J. A. (2021). A design science approach to developing an integrated mobile app forensic framework. *Computers & Security,* 105, 102226. https://doi.org/10.1016/j.cose.2021.102226