Received: 5.MAay .2024 Revised:1.Dec .2024 Accepted:15-.Dec.2024

Journal of Business Sustainability
Vol 2024., *No*1., DEC, 2024
https://jbs.zu.edu.jo/

CHANGING FACE OF DIGITIAL FORENSIC'S DUE TO IoT'S

Chander Mohan Gupta [1,2]

[1] Faculty of Management Sciences, Shoolini University of Biotechnology and Management Sciences, Himachal India
[2] Department Tax and Taxation, Tashkent State University of Economics, Tashkent, Uzbekistan.

Corresponding Author Email: cg30aug@yahoo.com, https://orcid.org/0000-0003-4855-8823

https://jbs.zu.edu.jo/

ABSTRACT

This Global development has come a long way, and the way it is going, it will not take much time to take over the world by storm. The way the usage of computers and the internet has grown was not enough that the new wave to an internet of thing (IoT) came in and has changed the way we have always seen the internet and its working. Trillions of G.B of data are being generated daily, and the same data is being interpreted and analyzed to provide new and innovative solutions to day-to-day problems. This information can be used positively or negatively, and it depends on the person who is using the data and the intentions with which it is being used. This information can be used to fight the new wave of crime by law enforcement agencies worldwide, and the same data can be used by financial institutions and firms to make big decisions in making the world a better place. IoT has come in as a tool to help and assist law enforcement agencies and prosecutorial offices with a series of guidelines that are in line with the rules and regulations laid down by the law to complete the investigation process. In the said manuscript, the authors have attempted to understand the role of IoT in the investigation process of digital crimes and tried to understand the reason for the lag in the judicial system in India and how this can be changed when law agencies and IoT shake hands and work together for a common goal. research themes, clusters, and interdisciplinary collaborations, advancing knowledge and informing future research directions.

Keywords:
Internet of Thing, Investigation, Digital Investigation, Investigating agencies and Law enforcement.

2. INTRODUCTION

Received: 6 April .2024 Revised: 1.Dec.2024 Accepted:15.Dec.2024

INTRODUCTION

The Iot, a synonym for the internet of things, is a combined technology of connecting physical electronic goods to the internet or cloud(Rasooli, Bhushan, & Kumar, 2020)(Tawalbeh, Muheidat, Tawalbeh, & Quwaider, 2020). The role of these physical products is to analyze the collected data on the problem; this is done without the individuals' interference as they reduce the usage of human interface in the process. When we break the Iot, I stands for the" internet" services commonly known as the world wide web and the connectivity of computer products, and the T stands for the "things," which are the physical products that can be as small as a wearable electronic watch. The primary purpose of IoT is the collection of data about the assigned job; it can be health care, agriculture or even meditation, and complex items like pollution, unemployment, diseases, and crime(Gercke, 2012; Morgan, 2019; Nouh, Nurse, Webb, & Goldsmith, 2019).

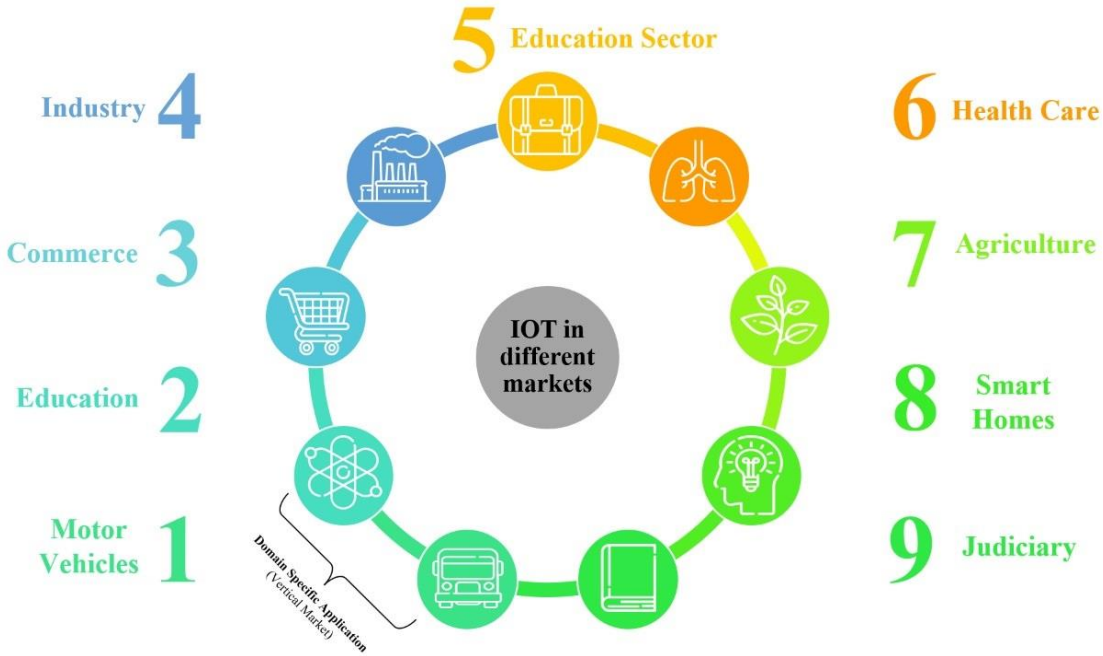

Fig: I Different areas where IoT can be/is used.(Developed by Author)

Digital/ Forensic investigation has been recognized as an academic and professional discipline in developed countries like the USA, U.K., Australia, and Germany, several courses at U.G. and P.G. level in these countries are being offered to the students, and the same has been famous as there are job opening available after successful completion of these courses, giving a push to the students in these countries to opt for the same (Tawalbeh et al., 2020) When we see into the working culture and style of the crime investigation there is a well-defined infrastructure that supports crimes, may it be traditional crimes or the new age cyber-crimes. This infrastructure is working at the state and national level and for both the public and private sectors. There is specific, explicit legislation that talks about the crimes that have been committed by misusing the internet, computer, and IoT, which are provided under the guidelines of the digital evidence. With the increase in IoT and other internet tools, this game has changed to another level. The underdeveloped country like India, Bangladesh, and others need to develop a unique digital forensic investigation infrastructure as India took many measures after the 2008 Mumbai attack (Chandran. R, 2021). After the attack, many questions were rocked at the administration as the question where we are equipped to tackle such kind of attacks and why were the intels of U.S. intelligence ignored about the potential attack (Robertson. N, 2021), and if proper precautions and steps would have been considered many lives could have been saved. The primary question in the investigation was the excessive use of digital devices and how high-level planning was done to make the attack success, and yes, they succeeded, to open our eyes and create new ways to understand the new digital investigation techniques and increase the use of IoT in the same. The use of satellite phones, Direct inward dialing, GPS equipment's and other IOT was unearthed (Federation of American Scientists, 2021).

Several incidences after that have rocked the Indian national security may be the Hacking of Indian official websites, web pages, or websites of atomic research claimed by the hackers from Pakistan (Federation of American Scientists, 2021). The train bombing of 2006 was also an example of IoT being used to commit the crimes as I.P. address and masking those I.P. address plus making proxies for the same was an integral part of the attack. It proves that the Indian digital forensic investigation infrastructure and the people associated are at the initial stages, and a lot must be done in this regard. IoT has been in use for quite now but is subject to professionals working in a specific area. These can be termed the technology to connect the physical devices to the internet; a simple example can be a WiFi router (Point Software Technologies, 2019). IoT is being used as an important tool to pull digital crimes as it is impossible for anyone to enter the network of any induvial or company without breaking into the IoT first (Rani, Kumar, & Bhushan, 2019). The crimes committed are either using IoT totally or taking the help of the instruments as much as possible. These devices are easily connected to the internet, and the information shared is at a click of a button. We can find a large number of gadget are available which can be easily transported and can be kept hidden from the eyes of people(i.e., sunglasses with camera and recording, a pen with camera and GPS, and how can forget the wearable watches which comes with a lot of feature and the best or the worst feature is that it is always connected to the internet) making it impossible for the naked eyes to get hold of such things. Until these things are being used for the benefit of the people, it is good, but if used for malicious activities, it damages the economy. The beauty of IoT is such that it can be used and misused in any field and any sector; the central point is that is its target audience and the mindset of the user, this can be used in agriculture, education, health care, and all the fields you name it and IoT is present there (Bhatt, Sharma, Sharma, Sharma, & Sharma, 2021). Thus, in the said study, the authors have tried to understand the working of IoT and digital forensic investigation and the infrastructure working in India with particular reference to academic structure, legal bodies, and law enforcing bodies(Sharma & Kumar, 2020).

S.No	Name of author/authors	Findings
1	Almuhammadi, S., & Alsulaiman, F. (2022)	This paper reviews digital forensic methodologies tailored for IoT-based healthcare systems, highlighting the challenges and solutions specific to this domain.
2	Conti, M., Dragoni, N., & Lesyk, V. (2022)	It provides a comprehensive survey of man-in-the-middle attacks in IoT environments, discussing the implications for digital forensics.
3	Sikorski, R., & Faber, S. (2023)	This paper discusses the various tools and techniques available for the forensic analysis of IoT devices.
4	Zhang, Z., & Wang, Y. (2023)	The focus is on the unique security and forensic challenges posed by smart home environments
5	Kumar, R., & Singh, S. (2024).	The authors propose advanced frameworks to address the specific needs of digital forensics in IoT ecosystems
6	Patel, N., & Chawla, S. (2024)	This research explores the integration of blockchain technology to enhance the reliability and traceability of digital forensic processes in IoT systems.
7	Hossain, M., & Karim, A. (2023)	A review of how machine learning techniques can be applied to digital forensics in IoT environments.
8	Rahman, A., & Ahmed, S. (2022).	This systematic review identifies the main challenges in IoT digital forensics and proposes strategic solutions.

9	Li, X., & Zhou, Z. (2023)	This paper provides a state-of-the-art review on the forensic readiness of IoT devices.
10	Wang, Q., & Liu, H. (2024).	An exploration of the frameworks and challenges associated with digital forensics in industrial IoT settings.

Table1: discussing the past research on the IOT and forensic accounting.

.

LITERATURE REVIEW

The widespread use of the Internet of Things (IoT) has had a tremendous influence on the field of digital forensics, creating both potential and difficult obstacles (Stout & Urias, 2016). With the increasing prevalence of IoT devices in our everyday lives, they provide a vast amount of data that is essential for investigations and incident response. Nonetheless, the decentralised and diverse structure of IoT ecosystems presents distinct challenges in gathering, safeguarding, and examining this digital data. (Hillier & Karroubi, 2022).

Researchers acknowledge the challenging responsibility of overseeing Insider Threat Detection in organisations, since malevolent actions might easily evade detection within the extensive network of IoT devices and the constantly growing digital traces (Hillier & Karroubi, 2022). The integration of the digital realm into the physical environment of the Internet of Things (IoT) has introduced hitherto unforeseen forms of assaults. These attacks need the development of a new, efficient, and widely distributed technique for detecting them. This is because IoT systems have limited resources and complicated architectures.

In order to tackle these difficulties, several researches have investigated the possibility of using machine learning and deep learning methods for intrusion detection in IoT-focused environments. These researches have shown encouraging outcomes in terms of scalability, precision, and decreased computing burden, providing a ray of hope in the competition to protect the more susceptible IoT environment.

The increasing reliance on IoT devices has generated significant security apprehensions, since the potential risks to these applications are continuously appearing and evolving. The following table is what gives an insight to the topic:

RESEARCH METHODOLOGY

The author of the article attempts to present the notion of digital/forensic investigation and its transformation as a result of the growing use of IoT technologies. The author has considered the law that governs these rules and regulations, which have been established and are now being implemented in the specified manner. The rules and regulations serve as both a standard and a checklist, guiding the authorities that implement them to ensure that the law is both effective and easily understood. The police officials and legal professionals are the only ones now working in this subject, which is why this task is being carried out.

Result and Analysis

The results and analysis are categorised into many sections. The first section focuses on comprehending the law, followed by the second section which examines the guidelines. The third section delves into the structure and operations of the Police Organisation, while the last section explores the efforts made in education and training.

Legislation:

Specific cyber offenses, digital signatures, and electronic records were recognized as a criminal act by the Information Technology Act 2000(I.T. Act, 2000), monitored by the ministry of communication and Information Technology. Section 66 of the Act defines hacking as an act of altering electronic information in some way or other to misuse it; Sec 67 talks about the publishing of obscene content which is an electronic form, but the problem comes when to implement all these as there are many loopholes in the system and lack of awareness among the people(Contents, 2019) many questions were raised in the case of Avnish Bajaj, CEO of Baazee.com as a lot of confusion and ambiguities were found (Symantec, 2019). These limitations led to the amendment of this act

in 2008, which redefined Hacking as a criminal activity. However, criminal acts are being covered under the Indian Penal Code 1860, and wherein the civil issues are dealt with by the Central Government adjudicating Officer who has been provided with the power of the civil court, which authorizes them to penalize pass judgment following the I.T. Act, 2000. The appeal of the same can be filed in the Cyber Regulations Tribunal. The investigation process of the same is a complicated affair which can either be done by the officials and if not in their domain this can be handed over to the private investigating agencies, as the type and level of crimes have gone up with the increased usage of IoT. Sec 78 gives in the details of the investigating officer who must not be below the rank of Deputy Superintendent of Police (Government of India, 2000), the reason for being the position gives him access to a larger area, and many police stations come under him which provides him with the freedom to work quickly and efficiently.

On the other hand, he can be held liable for the progress also. In 2009, the act was revised, giving the power of investigation to the Inspector in case of cybercrime because the number of issues was increasing, and the investigation was lacking behind (Government of India, 2009). Another major announcement in the amendment was that the number of cybercrimes centers was increased to divide the workload, and quick actions could be taken on the offenders. It was also found that the police officers lacked understanding of the Indian Penal Code (Scheidt & Adda, 2020), and the business sector reported the same, as the cybercrimes significantly hit them. Another angle to this was that the business community was afraid of brand devaluation and loss in profit due to such cybercrime attacks, and if taken care of the public, they have been fearful of reaching out to police due to the past experiences of harassment and non-action (Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, & Unodc, 2013). Sec 45 of the Indian evidence act ask for the testimony by the expert standing as a witness that they are an expert in the related field and have perfect knowledge about the topic in concern as the movement the use of IoT is there in the crime the witness needs to justify the capability of the instrument in questions and the capacity of the offender to pull that crime. With the increase in usage of IOT's communicating with each other, the chances of data breach and theft have increased manifold. Sec 43 of the ITA (amended) talks about*" **Reasonable practices and procedures and sensitive personal data or Information Rules, 2011" (Rules).*** However, the role of the private digital investigator as a witness is questionable; this does not mean that the police investigators cannot take their help; the legal provision provides them authority to outsource the investigation if needed.

Guidelines:

Now let talk about the implementation of the legal framework, our law is still in the initial stages, and a lot must have changed us as the recognition and prosecution of the cybercrime offenders, as there is still a gap between the law and its execution, plus the lack of specialized people to work with the authorities also creates a bend in the system. When compared to the Us and U.K. where NIST and ACPO, respectively. These organizations provide guidelines to the enforcement agencies, and India does not have such a body working here. Section 154-176 of the code of Criminal Procedure in support of Sec 80 of the I.T. Act, 2000 specifies the powers of the police department, but the point of concern is that there are no guidelines on the investigation of Cybercrime. The usage of IoT has further increased the complexity of the problem and needs to have more strict investigation guidelines. The amendment act 2008 gives more flexibility to the states and can develop and implement the rules and infrastructures to implement their investigation team and Modus of Operandi, which is to be recorded in the police manual of the state (Gercke, 2012). In the U.S., if the guidelines are not available, there is a CERT-IN (Computer Emergency Response Team), which is to be approached if the responder must follow as detailed by the American Federal Law Enforcement Training Centre (U.S. Department of Homeland Security, 2006). In India, CBI has been working with legal enforcement agencies is working on the investigating process concerning the working on cybercrime (CBI Crime Manual, 2005) with the collaboration Centre for development of Advanced Computing (CDAC) to increase the efficiency of the work drafted(Resource Centre for Cyber Forensics, 2021). The advancement of the work in this field is much to be done, and a lot must be achieved as there is not a single point of investigating authority, which leads to confusion, delays, and inconsistency in the investigation process. The rules change with the jurisdiction of the state, the investigation

officer changes, and many formalities are there, resulting in delay and sometimes forgoing the investigation process. (https://www.google.com/processofdigitalforensics&chips, 2018)

Police Organisation:

Guidelines issued by law enforcement agencies and the infrastructure seeking into the working of investigation in India lead to a significant discussion in India. In India, the police system is split into 2 tier organizations, the central and the state. The police are controlled differently at the state and center levels. The central team has access to 2 armed forces, and the other non- paramilitary organization such as CBI, is working in India, and other investigating agencies are there to support. (CBI. Central Bureau of Investigation, 2020).

Director-General of Police who heads the state police force is supported by Inspector General, Deputy Inspector generals, Superintendents, Deputy Superintendents, and Inspectors at the hierarchy level. CBI is vested with special powers and responsibilities when it comes to investigation, as they are given the charge of national-level crimes such as corruption, financial crime, bribery at the top level of administration, terrorism, and interstate crimes (CBI. Central Bureau of Investigation, 2020); additional work of supporting the different state-level investigations. Central Forensic Science Laboratory (CFSL) is also a part of CBI which seeks into the computer forensics division, whose main aim is to provide forensic support to the different bodies such as expert testimony, forensic services, on-site investigation support, and collection of evidence for the crime scene, plus giving training to the other bodies (CBI. CBI Crime Manual, 2005). India, a member of Interpol (Brown, 2015), has also given several insights to the investigating agencies in the area. Interpol's 7th International conference on Cybercrime held in New Delhi (Gercke, 2012) was also on the new trends on cybercrime and how there is a growth in the procedure. Interpol and CBI work hand in hand when a crime is investigated, in more than two countries, one being India. It also happened in the case of the Mumbai Attacks wherein Interpol, CBI, and international agencies such as the FBI was a part of the investigating team, and they were given unprecedented access to the evidence and the resources to find the truth behind the attack (Salamh & Mirza, 2021). Computer Emergency Response Team (CERT) is another wing that supports the investigating agencies in India about computer security incidents and gives advice on security issues (Point Software Technologies, 2019), this is the team that offers an insight into IoT and how they work, but they are not directly involved in the digital forensic investigation. There are several gaps in the system and the working bodies as sec 66 and 67 of the Information Technology Act of 2000, which talks about the investigation but is absent about the procedure and requirement of the forensic team, leading to help the private players enter into the investigation process as the law bounds them. They can enhance their digital forensic investigation services to any level and provide private players(Husamuddin & Qayyum, 2017; Ics-, 2021; Of, 2007). Several private players have entered the system of forensic investigation and doing tremendously well and providing professional guidance needed by the corporates, further enhancing their expertise in the legal side and other addon services(Al-room, 2021; Leloglu, 2017). That can be concluded that state police departments outsource the investigation work to these private players (Bhatt et al., 2021; Tawalbeh et al., 2020).

Education and Training:

The complex nature of the higher education system (HES) prevalent in India is much more complex than the same in the U.K. and U.S. In India University Grants Commission (UGC) is the one that is taking care of the higher education sector in India under the UGC Act, 1956. The commission's main objective is to control and maintain the different academic standards maintained by the HES in India (UGC, 2007). The Education Institutes (Universities) are being categorized as:

1. Central Universities are established by the central government act, passed by the parliament.
2. The state statute establishes State-level universities.
3. Deemed universities are those which are neither governed by center or state but are recognized by UGC.
4. Self-financed/ privately funded universities that are recognized by UGC are known as Private universities.

The problem arises that the degrees issued by the Higher Education Institutes that are not recognised are also not by the countries like the U.K. and USA (Acharya S. 2008). One reason for the same is the absence of a central admission authority in India as it is

in the U.K., this is the portal that allows the admission seekers to fill in the application, and then it is the central authority that redirects the applications, or the universities shortlist the students at the main level. This allows the process to be quick and effective, making it through direct inquiry or courses offered. If this system comes into the act in India, it will be a better way for a student to choose his approach based on their credentials. When it comes to forensic sciences courses, the same has been offered in India since 1952; thought the efforts of making it an entire-fledged approach started in 1967 when UGC and CBI came together to develop a course under a committee for establishing Criminology and Forensic Science (CFS) in Academia, these were to be affiliated to different universities and thus proper course to be seamline, Institute of Criminology and Forensic Sciences(ICFS) founded in 1971, with a significant objective to train a specific person in the field of forensic investigation. The University of Patiala and Madras started the degree courses for both U.G. and P.G. students under the head, leading the same to be established discipline, and the same started in the affiliated colleges. But same is not the case with Digital Forensics Investigation, as it has still not been identified as a specific discipline in India. There are just a handful of institutes that have considered this topic as a primary requirement of which Madras University's Criminology department offers M.SC in Cyber Forensics and Information Security (CBI, 2010), and SRM University is offering M.Tech in Information Security and computer forensics (CBI, 2007;). With time the number of HEI offering cyber investigations has gone to 256. Different training and refresher courses have started in India, and from police department to Army personal, such training is being provided to each government servant. The usage of such as take a lot of effort and time to make it available so that people can be aware of the facts and figure of Cyber investigation.

REFERENCES

1. Acharya S. Cyber terrorism-the dark side of the web world. Legal Service India. [Online]..Available from: http://www.legalserviceindia.com/ article/l169-Cyber-Terrorism.html; 2008 [accessed 20.03.21]
2. Almuhammadi, S., & Alsulaiman, F. (2022). Digital forensics for IoT-based healthcare systems: A review. Computers & Security, 110, 102476.
3. Al-room, K. (2021). Drone Forensics : A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. 13(1). https://doi.org/10.4018/IJDCF.2021010101
4. Bhatt, H., Sharma, B. B., Sharma, A., Sharma, R., & Sharma, M. (2021). An IoT-Based Soil Properties Monitoring System for Crop Growth and Production. 200–219. https://doi.org/10.4018/978-1-7998-7756-1.ch009
5. Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55–119. https://doi.org/10.5281/zenodo.22387
6. Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, & Unodc. (2013). Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, (February), 1–320. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
7. Contents, T. O. F. (2019). Now continued as Forensic Science International : Digital Investigation . AUTHOR INFORMATION PACK. 1–16.
8. Conti, M., Dragoni, N., & Lesyk, V. (2022). A survey of man-in-the-middle attacks in the Internet of Things. Journal of Network and Computer Applications, 87, 48-69.
9. Gercke, M. (2012). Cybercrime Understanding Cybercrime : Understanding Cybercrime: Phenomena, Challenges and Legal Response, (ITU), 366. https://doi.org/10.1088/1367-2630/11/1/013005
10. Hossain, M., & Karim, A. (2023). Machine learning in IoT digital forensics: A comprehensive review. IEEE Access, 11, 11234-11248.
11. Hillier, C., & Karroubi, T. (2022). Turning the Hunted into the Hunter via Threat Hunting: Life Cycle, Ecosystem, Challenges and the Great Promise of AI. *arXiv preprint arXiv:2204.11076*.

12. Husamuddin, M., & Qayyum, M. (2017). Internet of Things: A study on security and privacy threats. 2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017, (March 2017), 93–97. https://doi.org/10.1109/Anti-Cybercrime.2017.7905270
13. Ics-, P. (2021). 3 rd International Conference- IC4S-2021 Scheduled to be held on Proceedings of IC4S-2021 will be indexed in DBLP and Scopus Springer Lecture Notes in Networks and Systems (LNNS). 2021, 2–4.
14. Kumar, R., & Singh, S. (2024). Advanced digital forensics frameworks for IoT ecosystems. Future Generation Computer Systems, 137, 268-283.
15. Leloglu, E. (2017). A Review of Security Concerns in Internet of Things. Journal of Computer and Communications, 05(01), 121–136. https://doi.org/10.4236/jcc.2017.51010
16. Li, X., & Zhou, Z. (2023). Forensic readiness of IoT devices: A state-of-the-art review. Forensic Science International: Digital Investigation, 45, 301178.
17. Morgan, S. (2019). 2019 Official Annual Cybercrime Report. 2019 Report by Cybersecurity Ventures Sponsored by Herjavec Group, 12.
18. Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. (February). https://doi.org/10.14722/usec.2019.23032
19. Of, O. L. E. (2007). R Ole of I Matinib in.
20. Patel, N., & Chawla, S. (2024). Integrating blockchain with digital forensics for IoT. Computer Communications, 181, 120-130.
21. Point Software Technologies, C. (2019). Cyber Attack Trends Analysis Report. 01.
22. Rahman, A., & Ahmed, S. (2022). Challenges and strategies in IoT digital forensics: A systematic review. Journal of Computer Networks and Communications, 2022, 9867563.
23. Rani, D., Kumar, N., & Bhushan, B. (2019). Implementation of an Automated Irrigation System for Agriculture Monitoring using IoT Communication. Proceedings of IEEE International Conference on Signal Processing, Computing and Control, 2019-Octob, 138–143. https://doi.org/10.1109/ISPCC48220.2019.8988390
24. Rasooli, M. W., Bhushan, B., & Kumar, N. (2020). Applicability of wireless sensor networks & IoT in saffron & wheat crops: A smart agriculture perspective. International Journal of Scientific and Technology Research, 9(2), 2456–2461.
25. Salamh, F. E., & Mirza, M. M. (2021). UAV Forensic Analysis and Software Tools Assessment : DJI Phantom 4 and Matrice 210 as Case Studies. 1–14.
26. Scheidt, N., & Adda, M. O. (2020). Framework of Confidence Values during Digital Forensic Investigation Processes. 15, 228–234. https://doi.org/10.37394/23203.2020.15.24
27. Sharma, B. B., & Kumar, N. (2020). Internet of things-based hardware and software for smart agriculture: A review. Lecture Notes in Electrical Engineering, 597, 151–157. https://doi.org/10.1007/978-3-030-29407-6_13
28. Sikorski, R., & Faber, S. (2023). Forensic analysis of IoT devices: Tools and techniques. Digital Investigation, 34, 200-215.
29. Symantec. (2019). ISTR Internet Security Threat Report 2019 Volume 24. 24(February), 61. Retrieved from https://img03.en25.com/Web/Symantec/%7B984e78e2-c9e5-43b8-a6ee-417a08608b60%7D_ISTR_24_2019_April_en.pdf?elqTrackId=46f944879fdc4704ad360aae3cd0268e&elqaid=6820&elqat=2
30. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). applied sciences IoT Privacy and Security : Challenges and Solutions. Mdpi, 1–17.
31. Wang, Q., & Liu, H. (2024). Digital forensics in industrial IoT: Frameworks and challenges. Internet of Things, 15, 100291.

32. Zhang, Z., & Wang, Y. (2023). Security and forensic challenges in smart home environments. Journal of Information Security and Applications, 62, 102935.
33. https://www.google.com/processofdigitalforensics&chips. (2018). Digital Forensic Investigation Process (Vol. 18). Vol. 18. Retrieved from https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjMkPa6kdndAhVotosKHU1wAN0QjRx6BAgBEAU&url=https%3A%2F%2Fslideplayer.com%2Fslide%2F11865031%2F&psig=AOvVaw0gIaJL1M_48wQhrCdOQMDg&ust=1538066689809092
34. https://www.google.com/processofdigitalforensics&chips. (2018). Digital Forensic Investigation Process (Vol. 18). Vol. 18. Retrieved from https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjMkPa6kdndAhVotosKHU1wAN0QjRx6BAgBEAU&url=https%3A%2F%2Fslideplayer.com%2Fslide%2F11865031%2F&psig=AOvVaw0gIaJL1M_48wQhrCdOQMDg&ust=1538066689809092
35. Rotter, A., Barbier, M., Bertoni, F., Bones, A. M., Cancela, M. L., Carlsson, J., ... & Vasquez, M. I. (2021). The essentials of marine biotechnology. *Frontiers In marine science*, *8(1)*, 1-53.
36. Roy, A. (2019). Blue economy in the Indian Ocean: Governance perspectives for sustainable development in the region. *ORF Occasional Paper*, *1-38*.
37. Uddin, S. A., & Islam, M. M. (2019). Blue biotechnology, renewable energy, unconventional resources and products as emerging frontiers at Sea. *Journal of Ocean and Coastal Economics*, *6*(2), 1-26.
38. Wang, L., Niu, W., Ding, L., & Zhao, Z. (2023). A bibliometric review on marine economy: Current status, development and future directions. *Marine Policy*, *155(9)*, 1-22.
39. Yan, L., & Zhiping, W. (2023). Mapping the literature on academic publishing: a bibliometric analysis on WOS. *Sage Open*, *13*(1), 1-16.
40. Zhong, C., Li, T., Bi, R., Sanganyado, E., Huang, J., Jiang, S., ... & Du, H. (2023). A systematic overview, trends and global perspectives on blue carbon: A bibliometric study (2003–2021). *Ecological Indicators*, *148(4)*, 1-11.