JCBI
Journal of Computing & Biomedical Informatics Volume 02 Issue 02
ISSN: 2710 - 1606 2021

Review Article

Privacy challenges in cyber security against cybercrime in digital forensic. A systematic literature review in Pakistan.

Omer Aziz[1], M. Abdullah Siraj[2] and Abdul Rehman[3]

[1]Department of Computer Science, NFC-Institute of Engineering & Technology Multan, Multan, Pakistan
[2]Institute of Avionics and Aeronutics, Air University, Islamabad, 44230 , Pakistan
[3]Department of Information Technology, Virtual University, Lahore, 58000, Pakistan
[*]Corresponding Author: M. Abdullah Siraj. Email: malik.abdullah185@gmail.com

Received: March 07, 2021 **Accepted:** August 10, 2021 **Published:** September 15, 2021

Abstract: Cybercrime is a criminal activity that either target or uses a computer network or a network device. IOT become the biggest domain in these days.it is difficult to adopt digital forensics tools in IoT but somehow digital forensics play an important role in cyber security of IoT. Privacy and security challenges are increased day by day in digital forensics. Cybercrime in cyber security is increased day by day in digital forensics. Privacy and security are relate with each other but difference is that privacy relate to any right you have to control your personal information and how it's used. Lots of work has been done in security issue but less focus on privacy. In the recent year, privacy in cyber security is the biggest challenge against cybercrime in digital forensics. To overcome these challenges of privacy in cyber security we must have deep knowledge which threats and attacks are harmful of our network.in this article we discuss the current privacy threats and attack for cybercrime in digital forensics with the deep knowledge and proposed classification matrix and also define proposed system which control threats and attacks. To the best of our knowledge there is no survey on privacy challenges in cyber security against cybercrime in digital forensics.

Keywords: Cyber Security; Privacy; Security Cybercrime; Digital Forensics.

1. Introduction

Nowadays, in computer science field the current trend refers to big data. This paper focused on privacy and security on the internet so that every person feels free and comfortable while working on the network. Purpose of this paper is to describe the privacy challenges in cyber security against cybercrime in Pakistan. Digital forensics uses scientific methods to analyze and interpret electronically stored information (ESI) to reconstruct events (Wang & Alexander, 2015). Digital forensics software enables to analyze any information that is on a computer or over a network (Wang & Alexander, 2015) Digital forensics (DF) software development is different from that in other areas (Wang & Alexander, 2015) The difference lies in data scale, data diversity, human capital, temporal diversity, and the crime scene investigation effect (called CSI effect) (Wang & Alexander, 2015)

Cybercrime is any kind of crime that can be done in, with, or against networks and computer systems (Wang & Alexander, 2015) Privacy and security are related with each other but difference is that privacy relate to any right you have to control your personal information and how it's used. Security on the other hand refer to how your personal information is protected. Purpose of this paper is to describe the challenges of privacy in cyber security in digital forensics.

In the research paper (Wang & Alexander, 2015) the author defines the security issue in detailed but less focus on privacy. Privacy is also an important feature in big data. In big data there are a lot of issue related cyber security in digital forensic.

Data come in high speed sometimes a person that does not have technical knowledge cannot tackle the high speed of data and ignore various threat in data that cause the privacy attack. In the rest of the paper, you can find the basics issue that cause privacy attack or also find the future prediction for cyber security against cybercrime in digital forensics.

1.1. Related work

In the previous paper author, more focus on security of cyber security against cybercrime. Some of the paper describe privacy issues.in previous paper author wrote about privacy trend and future. author wrote image forensics, file forensics, memory forensics etc.

In a computer system, Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. (Dezfoli et al., 2013) In this paper author describe forensics investigation tools such as P2P and it's based on JAVA Serialization but this tool used for law enforcement community. Another tool such as pay flag uses html files but it also has some privacy issue so it not available openly. The author describes the method of Strategy of Triple-E (Seton) which is used to crack a password in solving Trojan defense in cybercrime (Dezfoli et al., 2013)

Honeypot is a computer system running on internet which design to trick other people who attempt to illegally break network but this method needs more time and also has some security risk. Some forensics use fingerprint device. clock skew is a unique identifier but this approach has some gaps such as it will not possible to perform the measurement if the option has been taken by the device. This paper is more focus on a privacy challenge. Most of the challenges are lack of technical language, change of government. In this paper we focused what are main cause of lack in privacy in digital forensics.

2. Materials and Methods

This review is taken as systematic literature review. the step in systematic literature review is taken as below:

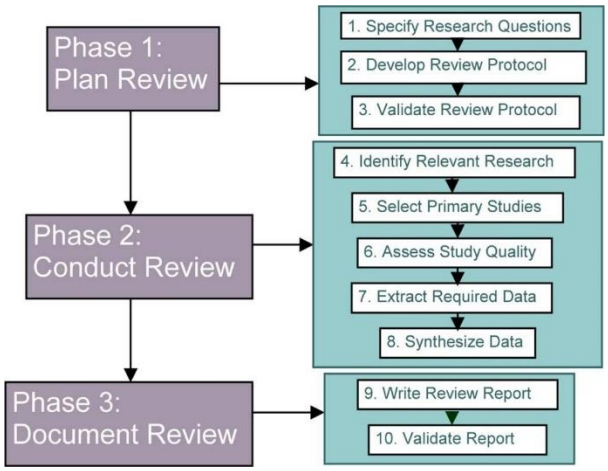

Figure 1

2.1. Aims and objective

To isolate the concept of main issue in privacy of cyber security in digital forensics. To identify different attack that harmful of our network.

2.2. Research question

Q1 what are privacy challenges in cyber security against cybercrime in digital forensics?

Q2 which types of threats and attacks affect our network?

Q3 what are current limitation?

2.3. Searching the literature

I have searched the literature from following database.

Table 2

Source	Type of paper
ACM digital library	review paper
IEEE Xplore	SLR paper
ELSVIER	SLR
Science direct	conference
springer link	review paper

ACM digital library, IEEE Xplore, ELSVIER, Science direct, springer link

2.4. Inclusion

- Articles written in English are considered
- Cyber security related research paper
- Digital forensic related paper includes
- Research paper from 2015 to 2020 are to be considered

2.5. Exclusion

- Paper related to IOT cyber security exclude
- Paper related to fraud detection in credit card

Paper related to cyber security in other system are exclude.

In many paper authors describe security issue but privacy issue is still needed to be focused.

- Lack of technical knowledge
- Changing of government
- Making copyright
- A person moral value
- Lack of human computer interaction

Answering Q# 2, 3

Table 3

Types of attack	In business	In personal account
Virus	30%	30%
Malware	30%	10%
e-mail hacker	60%	40%
Trojans	40%	10%

3. Classification table

	year	Technology used	Problem tackled	Audience tackled	Criteria A1	Criteria A2	Criteria A3	Criteria A4	Total score
[1]	2017	IOT sensor, UAVs, BAS	Digital forensics investigation in the context of smart cities	Smart cities	1	1	0.5	1	3.5
[2]	2018	Industrial internet of things, sensor	Cyber security in manufacturing system	Smart industrial areas	0.5	1	0.5	0.5	2.5
[3]	2016	Digital forensics with IoT	Finding the missing piece of IoT in digital forensics	Forensics practitioners, device manufactures and legal authorities	1	1	1	1	3
[4]	2018	Anti-forensics techniques (Cryptographic and steganography)	Analysis of digital forensics in cyber security	Researchers, Users	0.5	0.5	0.5	1	4
[5]	2014	Privacy issue in EU,US and APEC privacy regulation	Privacy respecting in digital privacy issue	Generally(Protect data from attacker)	1	1	1	1	3
[6]	2016	Cloud and mobile forensics	Secure data from cyber attackers	Survey on cyber forensics	0.5	1	1	0.5	3
[7]	2015	Survey on Digital evidence smart devices	Survey on DF in smart devices based on OS file management	Digital forensics on smart devices	1	1	0.5	0.5	4
[8]	2020	Forensics on Cloud or Forensics As a service	Legal privacy and cloud storage challenges	DF based IoT solution for chain block chain based solution	1	1	1	1	4
[9]	2016	Digital Forensics investigation framework for IoT	It facilitate effective digital forensic crime investigation in IoT	Law enforcement community	1	1	1	1	3.5
[10]	2019	Specific application forensics for IoT application	Heterogeneous in IoT devices and lack of unified standard	IoT application-specific digital forensics investigation	1	0.5	1	1	3
[11]	2016	Cloud and mobile forensics	Privacy respecting in digital privacy issue	Cloud and mobile forensics	0.5	0.5	0.5	1	2.5

Figure 3: Clasiffication table.

In (Wu et al., 2018)author briefly describe attack which directly attacks our cyber security.

The current limitations are

- Rarely open-source software used for privacy in digital forensics.
- Need to be bench marking.
- There is also a need to people learn about their moral values.
- To overcome all these challenges, we must develop a system for this purpose. If a person involves wrong activities, he would not allow to login further and his request is rejected and caught at that point.

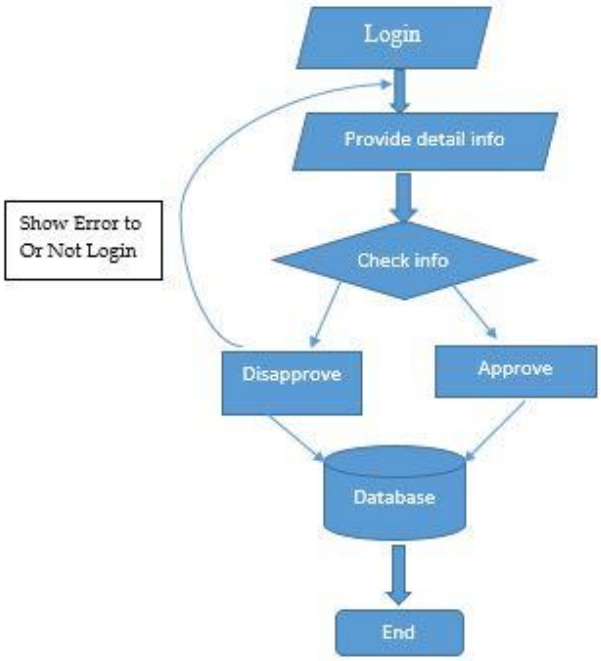

Figure 4

4.Risk

If a no of person login at the same time the website may slow down or privacy violation is still need to be more focused. For email forensics. Two methods are used. Content based analysis but this method is very time consuming. Event based analysis identify the pattern in which time email is sent and which person are involved. This method is more efficient than content-based analysis. In (Watson, Dehghantanha, & Security, 2016) author briefly describe the strategy of triple E to solving Trojan defense which is used to crack a password but now most of the digital forensics' software available openly so that it may come in to our mind that how to control the distribution of the open-source software from unethical person.

5. Result and discussion

In the 1st part I will give the answer of my research question which is Privacy and security are relate with each other but difference is that privacy relate to any right you have to control your personal information and how it's used. Security on the other hand refer to how your personal information is protected.

Privacy challenges and current limitation are change of government, moral values of a person, lack of knowledge, high cost etc. Some privacy systems are introduced for cyber forensic such as GDSPR but it's still rarely applied in Pakistan.

In previous research paper author talk about the security issue and its related threat and attack but not briefly describe privacy issue

Privacy is also important in digital forensics privacy relate to person itself.

In future there is a need to do more work on privacy violation and there is a need to do bench marking means there is a need to do comparison between the develop privacy system and others. scalability is also an important feature in privacy there is a need to scale the work of the people and then train them to do privacy in cyber security in digital forensic.

There is also a need to that government should make act for privacy such as California consumer privacy act its purpose to restrict how companies collect and use data making this type of act it's also reduce the cost that people are easily attract.

6.Conclusion

This study has been taken for finding the privacy challenges in cyber security in digital forensics. For conducting this we followed a systematic literature review. This review is based on almost 20 papers. We briefly study the previous paper and provide the detail in depth about security challenges in cyber security. After reading this paper we conclude that although many techniques have been developed and different models are used but all the techniques and models has some flaws .in this SLR we briefly describe developed models with their challenges. Furthermore, we also define taxonomy of attacks and viruses with their ratios in different fields also provide a solution to secure our data. Future direction for this work involves privacy scalability, privacy violation and benchmarking.

References

1. Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. J. I. J. A. C. S. A. (2018). Cyber-security incidents: a review cases in cyber-physical systems. (1), 499-508.
2. Attique, M., Farooq, M. S., Khelifi, A., & Abid, A. J. I. A. (2020). Prediction of therapeutic peptides using machine learning: computational models, datasets, and feature encodings. *8*, 148570-148594.
3. Baig, Z., Szewczyk, P., & Valli, C. Future challenges for smart cities: cyber-security and digital forensics. Digit. Investigat. 22, 3–13 (2017). In.
4. Dehghantanha, A., & Franke, K. (2014). *Privacy-respecting digital investigation.* Paper presented at the 2014 Twelfth Annual International Conference on Privacy, Security and Trust.
5. Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., Daryabar, F. J. I. J. o. C.-S., & Forensics, D. (2013). Digital forensic trends and future. *2*(2), 48-77.
6. Harichandran, V. S., Breitinger, F., Baggili, I., Marrington, A. J. C., & Security. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *57*, 1-13.
7. Kalaimannan, E. (2015). *Smart Device Forensics-Acquisition, Analysis and Interpretation of Digital Evidences.* Paper presented at the 2015 International Conference on Computational Science and Computational Intelligence (CSCI).
8. Kebande, V. R., & Ray, I. (2016). *A generic digital forensic investigation framework for internet of things (iot).* Paper presented at the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud).
9. Mehmood, E., Abid, A., Farooq, M. S., & Nawaz, N. A. J. I. A. (2020). Curriculum, teaching and learning, and assessments for introductory programming course. *8*, 125961-125981.

10. Obaid, I., Farooq, M. S., & Abid, A. J. I. A. (2020). Gamification for recruitment and job training: model, taxonomy, and challenges. *8*, 65164-65178.
11. Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., . . . Forensics, T. i. C. (2020). Current challenges of digital forensics in cyber security. 31-46.
12. Paul Joseph, D., & Norman, J. (2019). *An analysis of digital forensics in cyber security.* Paper presented at the First international conference on artificial intelligence and cognitive computing.
13. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E. K. J. I. C. S., & Tutorials. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *22*(2), 1191-1221.
14. Wang, L., & Alexander, C. A. J. D. T. (2015). Big data in distributed analytics, cybersecurity, cyber warfare and digital forensics. *1*(1), 22-27.
15. Watson, S., Dehghantanha, A. J. C. F., & Security. (2016). Digital forensics: the missing piece of the internet of things promise. *2016*(6), 5-8.
16. Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. J. J. o. m. s. (2018). Cybersecurity for digital manufacturing. *48*, 3-12.