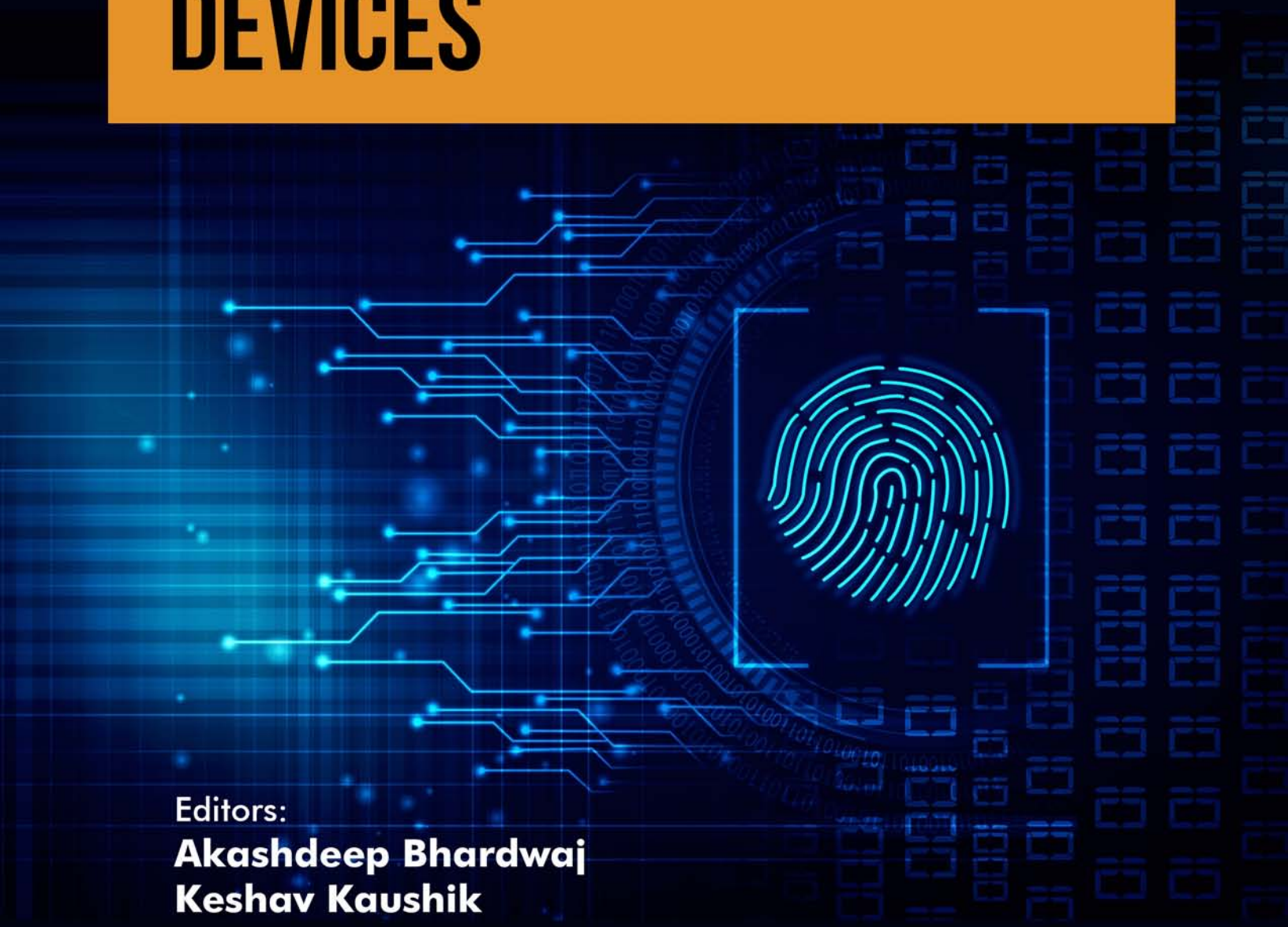
CYBER FORENSICS AND INVESTIGATION ON SMART DEVICES



Editors:
Akashdeep Bhardwaj
Keshav Kaushik

Bentham Books

Cyber Forensics and Investigation on Smart Devices

(Volume 1)

Edited By

Akashdeep Bhardwaj
Cybersecurity & Digital Forensics
University of Petroleum and Energy Studies
UPES, Dehradun
India

&

Keshav Kaushik
School of Computer Science
University of Petroleum and Energy Studies
Dehradun
India

Cyber Forensics and Investigation on Smart Devices

(Volume 1)

Editors: Akashdeep Bhardwaj and Keshav Kaushik

ISSN (Online): 3041-0983

ISSN (Print): 3041-0975

ISBN (Online): 978-981-5179-57-6

ISBN (Print): 978-981-5179-58-3

ISBN (Paperback): 978-981-5179-59-0

First published in 2024.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

Smart devices are now being commonly used by everyone in their daily lives for routine activities. These smart devices enable us to connect with others (smartphones), have driverless cars (smart cars), secure our buildings (smart locks), remotely control appliances in our homes (smart homes), and remind us to do things and do things for us (smart assistants like Alexa and Siri). At the personal level, wearables enable us to use these smart devices on our bodies and wear them like accessories or embedded in our clothing or implanted in our bodies. For example, we wear smartwatches and fitness trackers to keep track of our physical activities, our heart rate, and our quality of sleep. For healthcare, we use wearables to measure our temperature, blood pressure, breathing rate, blood sugar level, heartbeat rate, and brain activity and monitor our vital signs. Smart devices and wearables have become pervasive, but they need Internet or Network connectivity and Internet of Things infrastructure.

As smart devices, wearables, and implantable technologies get more traction in healthcare, we need to be mindful of their security because of their connectivity to the Internet. For example, pacemakers now have built-in WIFI connectivity for any adjustments that are required in the future. Next-generation cardiac wearables and other implantables will integrate into Wireless Body Area Networks (WBAN). Specialists will sit at their desktops, connect to these implantables *via* the WIFI, and make adjustments. Such connectivity poses security risks, and these risks are not only monetary losses but also losses of life if the implantables are sabotaged. Therefore, the security issues of these devices through cyber forensics and investigations are thoroughly explored in this edited book. The vulnerability of these devices is mostly during data transmission to the cloud or the owner's personal device with which it is paired. Blockchain-based security controls are now being implemented with two-factor authentication (2FA) by most device makers to mitigate against such security vulnerabilities.

As lives are at stake, we need to have a foolproof process to investigate and ascertain the intent of the cyber attackers and potential sabotages while gathering evidence to prosecute them and defend the devices from future attacks. The cyber forensics and investigation process is ideal as it allows investigators (depending on which standard you follow) to identify, obtain, process, and analyse data to report about the security incidents that took place to management for mitigation action and authorities for prosecution. As the smart devices are part of a network or connected *via* a wireless network, network monitoring is possible, and all the cyber security protocols can be applied to these smart devices, logs can be inspected, and all activities monitored for forensics. The cyber forensics and investigation process will encourage the adoption and use of smart devices such as the Internet of Things (IoT), Internet of Everything (IoE), and Internet of Bodies (IoB) to become pervasive. All these devices and things will sense, collect, process, and store huge amounts of data (big data) and will create unprecedented opportunities for us to investigate the evidence through the discipline of cyber forensics.

This book on cyber forensics and investigation on smart devices is a timely publication as we undergo digital transformations. Smart devices, wearables, and implantables are getting cheaper, powerful, and are able to handle many processes with network connectivity. With the proliferation of Internet of Things (IoT) devices, the attack surface area has dramatically increased for hackers and the threat surface area has significantly increased for cyber security specialists. This book covers the architecture, deployment problems, applications, data processing, storage, and review of Internet of Things (IoT) protection and privacy problems in a cloud-based approach. The main idea behind this book is to give a practical guide to readers that will cover the advanced tools and techniques used in the domain of cyber forensics and

investigation. I hope the readers find the book inspiring and gain a working knowledge of cyber security issues facing smart devices and the mitigation solutions that can be applied to prevent breaches. It is evident that smart devices will become ubiquitous and will become indispensable. The best we can do is learn to live with smart devices by identifying cybersecurity issues and mitigating them.

Sam Goundar
RMIT University
Melbourne
Australia

PREFACE

Cyber forensics and investigation on smart devices (CFISD) by Bentham Science is the brainchild of Akashdeep Bhardwaj and Keshav Kaushik. The focus of this book is to bring all the related managerial applications of cyber security and digital forensics to a single platform, so that undergraduate and postgraduate students, researchers, academicians, and industry people can easily understand. This edited book aims to provide the concepts of related technologies and novel findings of the researchers through its chapter organization. The primary audience for the book incorporates specialists, researchers, graduate understudies, designers, experts, and managers who are researching this domain. The edited book will be organized into independent chapters to provide readers with great readability, adaptability, and flexibility. Big thanks to all our co-authors, who are experts in their own domains, for sharing their experience and knowledge. This book is an attempt to compile their ideas in the form of chapters and share them with the world. This book provides insights into cyber forensics, cybercrimes, mobile forensics, cyber investigations, Internet of Things, smart home, smart devices, and sensors. The book will be helpful for security professionals, cyber forensic experts, academicians, scientists, advanced-level students, penetration testers, and researchers working in the field of cyber forensics and IoT. We would like to thank the contributors to this book for their smooth collaboration and Bentham Science Publishers.

Akashdeep Bhardwaj
Cybersecurity & Digital Forensics
University of Petroleum and Energy Studies
UPES, Dehradun
India

&

Keshav Kaushik
School of Computer Science
University of Petroleum and Energy Studies
Dehradun
India

List of Contributors

Ankit Vishnoi	School of Computer Science and Engineering, Manipal University, Jaipur, India
Abhishek K. Pradhan	School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
Devakrishna C. Nair	School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
Hitesh Kumar Sharma	School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007, India
Hemanta Kumar Bhuyan	Department of Information Technology, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Guntur, Andhra Pradesh, India
Hepi Suthar	Rashtriya Raksha University, Gandhinagar, India Vishwakarma University, Pune, India
Luxmi Sapra	School of Computing, Graphic Era Hill University, Dehradun, India
Lokaiah Pullagura	Department of Computer Science & Engineering, Faculty of Engineering & Technology, Jain Global Campus, Jain University, Kanakapura-562112, Ramanagara District, Karnataka, India
Manoj Kumar	School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007, India
Nalli Vinaya Kumari	Department of Computer Science & Engineering, Malla Reddy Institute of Technology and Science, Hyderabad, India
Preeti	School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007, India
Prabhu Manikandan V	School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
Tripti Misra	School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
Varun Sapra	School of Computer Science, University of Petroleum and Energy Studies Gurugram, India

CHAPTER 1

Smart Home Forensics

Lokaiah Pullagura[1,*], Nalli Vinaya Kumari[2] and **Hemanta Kumar Bhuyan[3]**

[1] *Department of Computer Science & Engineering, Faculty of Engineering & Technology, Jain Global Campus, Jain University, Kanakapura-562112, Ramanagara District, Karnataka, India*

[2] *Department of Computer Science & Engineering, Malla Reddy Institute of Technology and Science, Hyderabad, India*

[3] *Department of Information Technology, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Guntur, Andhra Pradesh, India*

Abstract: The Internet of Things (IoT) has unquestionably exploded into the forefront of everyone's lives, whether they realise it or not. Internet of Things (IoT) technology is now used in medical devices, transportation, and even in our homes. Devices such as these have the ability to access a great deal of personal information. Because of their diminutive size, these devices have made insufficient efforts to build security into their design. Sensors, cameras, and lights are all examples of Internet of Things (IoT) devices that can be used to automate daily tasks around the home. Smartphones and speakers can be used as remote controllers to operate these gadgets. A smart home's IoT devices collect and process data on motion, temperature, lighting control, and other variables, and they store a wider range of data from more diverse users. A wide variety of smart home devices can make extracting meaningful data difficult because of their differing data storage methods. Data from a variety of smart home devices, as well as data that can be used in digital forensics, must be collected and analysed. Google Nest Hub and Samsung Smart Things are the primary sources of forensic smart home data that will be analysed in this study. As a result, we analysed the smart home data collected using companion apps, web interfaces, and APIs to find information that was relevant to our investigation. Various types of data collected by smart homes are also discussed in the paper, and they can be used as crucial evidence in certain forensic cases. IoT devices in a smart home can be hacked, and we'll investigate how, what data can be recovered, and where it resides after it has been hacked as part of our investigation.

Keywords: Cybersecurity, Digital evidence, Digital forensics, Data analysis, Evidence collection, Forensics, Home automation, Internet of things (IoT), Investigative techniques, Smart home.

[*] **Corresponding author Lokaiah Pullagura:** Department of Computer Science & Engineering, Faculty of Engineering & Technology, Jain Global Campus, Jain University, Kanakapura-562112, Ramanagara District, Karnataka, India; Email: dr.lokaiah@gmail.com.

Akashdeep Bhardwaj & Keshav Kaushik (Eds.)

1. INTRODUCTION

Home owners can benefit from new internet-enabled devices that are easy and safe to use. The introduction of new internet-enabled devices, particularly at home, is seen as a convenient and safe way to enhance human life. A home's systems can be controlled, monitored, and even entertained using Internet-enabled gadgets. A “smart house” is comprised of gadgets like this one. Throughout this paper, we'll refer to these gadgets as the “Internet of Things” (IoT). A whopping $53 billion could be generated by smart home gadgets like smart plugs and switches, smart speakers, and surveillance camera systems by 2022 [1, 2]. Despite the rapid uptake of IoT devices in the home, there have been reports of cyber-attacks and privacy concerns [3, 4]. Avast [5] estimates that one out of every two Internet of Things (IoT) devices in smart homes is vulnerable to cyberattacks. IoT devices are ubiquitous in today's smart homes, making security and privacy a top priority. An estimated 75% of people say they don't trust their IoT devices when it comes to handling and sharing their personal information [6]. Smart homes have become increasingly popular due to their convenience and ability to automate various aspects of daily life. However, with this increased reliance on technology, there is a growing need for forensic investigation of smart homes in cases of security breaches, theft, or other criminal activity. Smart home forensics involves the application of forensic techniques to digital devices and networks that make up a smart home, including the analysis of data from devices such as smart speakers, thermostats, security cameras, and home automation systems, as well as the examination of network traffic and other digital evidence. Smart homes consist of various interconnected devices and systems that are controlled by a central hub or app [6]. These devices can include smart TVs, home security systems, smart thermostats, and even smart refrigerators. They are designed to make life easier and more convenient for users, but they can also create vulnerabilities that can be exploited by hackers and other malicious actors. Smart home forensics involves the use of forensic techniques to analyze digital devices and data in order to identify evidence of unauthorized access, data theft, or other criminal activity. This may involve the collection and analysis of data from various smart devices, such as security camera footage, device logs, and other digital data. Forensic investigators may also examine network traffic to identify unusual activity and potential sources of attacks. One of the challenges of smart home forensics is the lack of standardization in smart home devices and protocols. Different manufacturers use different technologies and standards, making it difficult to create a unified approach to forensic investigation. Additionally, the complexity of smart home systems can make it difficult to identify and analyze potential sources of evidence. Another challenge is the need for specialized tools and techniques for forensic analysis. Traditional forensic tools may not be sufficient for analyzing smart home devices and data, and investigators may need

to use specialized software and hardware tools to extract and analyze data from these devices. Despite these challenges, the importance of smart home forensics is likely to continue to grow as more people adopt smart home technology. Forensic investigators and other professionals will need to develop the necessary skills and knowledge to effectively investigate these types of cases and identify and prevent potential security threats [7]. An in-depth examination of forensic investigations into smart homes and the use of a laboratory to look into potential threats is provided. Both methods are described in great detail. The data from the IoT lab will assist us in answering the following research questions: There are a number of smart home devices and smartphone apps that can provide valuable information. How secure are these smart home gadgets when it comes to personal data? Does the security of these smart home devices need to be improved? For smart home devices, what are the best ways to collect and analyse data? These smart home appliances are exchanging what kinds of personal information. It's laid out like this: Section 2 provides background information on IoT forensics and Smart Home devices. Section 3 and Section 4 describe our smart home lab and the digital forensic investigative process. Threats to smart homes are discussed in Section 5 of this document. Finally, Section 6 brings an end to all of our hard work.

2. RELATED WORK

The Internet of Things (IoT) refers to the network of physical devices, vehicles, home appliances, and other items that are embedded with electronics, software, sensors, and network connectivity, allowing them to connect and exchange data. Smart home devices are a subset of IoT devices, specifically designed to automate and optimize the control of home appliances and systems [8]. The forensic investigation of IoT devices, including smart home devices, is an emerging field that involves the use of specialized techniques and tools to collect, preserve, and analyze digital evidence. The investigation of IoT devices typically involves a combination of network analysis, digital forensic techniques, and traditional investigative techniques.

One of the challenges of IoT forensics is the sheer number and variety of devices that are involved in a typical IoT system, including smart home devices [9]. The investigation of IoT devices requires specialized knowledge of the underlying technologies and protocols used by these devices, as well as an understanding of the data they generate and how it can be collected and analyzed. The forensic investigation of smart home devices involves the analysis of various types of digital evidence, including logs, network traffic, and data stored on the device itself. Smart home devices may generate a large amount of data, including audio and video recordings, environmental data, and user activity logs, all of which may

CHAPTER 2

A Guide to Digital Forensic: Theoretical To Software Based Investigations

Preeti[1,*], **Manoj Kumar**[1] and **Hitesh Kumar Sharma**[1]

[1] *School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007, India*

Abstract: Digital forensics is a part of forensic science that works with the use of digital data generated, saved, and communicated by digital devices as evidence in investigations and judicial actions. It is a growing field in computing that frequently necessitates the intelligent analysis of large amounts of complex data. A form of digital forensics has existed since nearly the invention of computers, however, as digital forensic processes have matured and needs have become more prevalent, forensic capabilities have seen significant advancements in recent years. Rapid advancements in computer science and information technology enable the development of novel techniques and software for digital investigations. Initially, much of the analysis software was unique and proprietary, but over time, specialised analysis software for both the private and governmental sectors became available. Also, it appears that Artificial Intelligence (AI) is an ideal approach for dealing with many of the current problems in digital forensics. It is a well-established branch of modern computer science that may help solve computationally massive or complicated problems in a reasonable amount of time. The goal of this paper is to deliver a high-level overview of digital forensics phases, applications, merits and demerits and widely used software of the domain. The paper also discusses legitimate and legal considerations followed by the scope and role of artificial intelligence for solving complex problems of digital forensics.

Keywords: Anti forensics, Cyber crimes, Digital forensic, Forensic tools, Forensic software.

1. INTRODUCTION

Across the globe, people and associations are racing to implement new advances to improve and grow in an increasingly interconnected world. The convergence of the technological progressions in informative technology, for example, cloud co-

[*] **Corresponding author Preeti:** School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007, India; Email: preeti.sharma@ddn.upes.ac.in

mputing, social networking, personal devices, for example, smart phones and so forth and the pervasive utilization of it worldwide have resulted in numerous benefits for humanity, yet it additionally gives roads to misuse and has presented new challenges for policing cybercrimes. Cyber-crimes or digital crimes have increased in frequencies with the advancement and more complex techniques being deployed by individuals and groups with intricate and advanced knowledge of the working of the internet, networks and security architectures, and who use their specialist skills for crimes, normally called the Dark Side of Internet. It presents significant implications and difficulties for national and economic security [1].

Many associations are at huge risk. This statement has been proved by the number of complaints received and processed for instance by Internet Crime Complain Centre (IC3) of the Federal Bureau of Investigation (FBI). In 2017, the total quantities of complaints received are 301,580 with reported losses of $1,418.7 million. In this report, India is at second number in the list of top 20 victim nations with 2,819 complaints. This is significant by additionally considering many personal and organisational data breaches and monetary losses go unreported in our nation and mostly complaints are by financial institutions like credit card organizations and banks. The list of top 20 countries by victim is depicted in Fig. (**1**) (sourced from https://www.bankinfosecurity.com/fbi-see--internet-enabled-crime-losses-hit-13-billion-a-10033)."

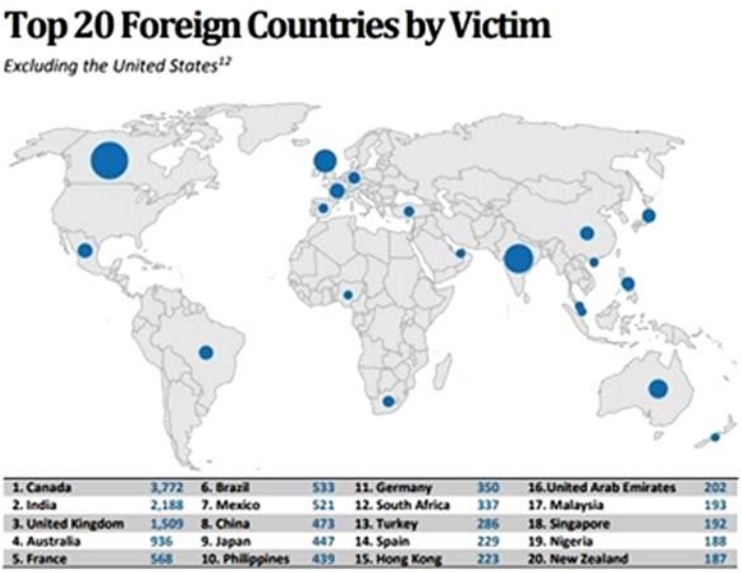


Fig. (1). List of Top 20 victim countries of cyber crime [1].

The number of incidents of cybercrime in India is rising pointedly. An IIT Kanpur study shows that the number grew from 71,780 out of 2013 to 1.49 lac in 2014 to 3 lac in addition to in 2015, in this way recording a yearly increment of more than 100% from 2014 to 2015. With the advent of various digital gadgets, the internet, and social media, the environment in which digital crimes are committed has fundamentally changed. It is currently insufficient to simply examine the victim's PC's hard drive, as additional evidence will be required for a successful prosecution of the perpetrator and determination of the root cause of the crime [2]. The latter is fundamental for know about the new methods utilized by criminals and accordingly modified the investigation as additionally the investigation of future crimes. The development of highly technical and sophisticated nature of digital crimes has made another part of science known as Digital Forensics. Because there were few specialized digital forensic tools available in the 1980s, investigators frequently performed live examinations on media, examining computers from within the working framework, and extracting evidence using existing system admin tools. This practice conveyed the risk of inadvertently or intentionally modifying data on the plate, which prompted claims of evidence tampering. In the mid-1990s, many tools were created to solve the issue. The chapter involves introduction, brief history, objectives of digital forensics in section 1. Section 2 discusses about its current issues followed by its various phases and categories in section 3 and 4. Section 5 and 6 introduce about various tools and software like FTK, QRadar, and Parrot securities *etc*. used for analyses of different forensic cases. Section 7 discusses about various advantages, disadvantages and applications of digital forensic. Section 8 defines legitimate and legal considerations of forensic field followed by section 9 that introduces the role of digital forensics in Artificial Intelligence. Finally section 10 concludes the chapter with discussion about future scopes of the forensic field.

1.1. Origin of Digital Forensics

In 1984, the FBI started creating tools to look at computer evidence, which is when the field of digital forensics was first born. To combat digital crime, digital forensic professionals acquire in-depth information, design specialized forensic software, and follow conventional methods from physical forensics. Computer crime is a significant criminal activity with rising incidence and frequency. Business organizations, law enforcement, and the government are all being put under pressure by this rise in illegal activities. Hence, a quick reformulation of standards and processes was required to move from document-based evidence to digital/electronic evidence. Many inquiry models have been put out over the years by various inventors.

CHAPTER 3

Cyber Forensic: End-to-End Secure Chat Application Value Beyond Claimed Encryption Method

Hepi Suthar[1,2,*]

[1] *Rashtriya Raksha University, Gandhinagar, India*

[2] *Vishwakarma University, Pune, India*

Abstract: The everyday rise in third-party applications across different app stores, mobile operating systems, mobile hardware, and application versions themselves has not only prompted but to a certain degree, necessitated the digital forensics community and digital forensics researchers to investigate various applications that are not inherently supported and parsed by commercial forensics tools. Apart from the capabilities associated with various forensic tools, depending on the case, many forensic investigators may come across the most unthought-of third-party applications for investigation. The only questions then would be: 1) How to parse such data? 2) Is there anything of forensic value? And 3) Some third-party application manufacturers claim that they encrypt data. However, due to the lack of time and technology, in some instances, when there is no access to or knowledge of the decryption method, where and how do find data pertinent to the investigation? Depending on the circumstances mentioned above, is it crucial to come to a firm conclusion about how and where some data resides for certain third-party applications, regardless of what the manufacturers claim. There is a plethora of third-party applications out right now that are utilized by people for a variety of purposes, whether it is for good or bad. Oftentimes, as forensics practitioners, it is our job to dig down and hunt for data that can give us some insight into what was going on in the device, related to a particular application. These applications may offer capabilities such as geolocations, communications, network-related artifacts, *etc*., that can be of value to certain cases.

Keywords: Chat application, Evidence, Encrypted message, End to end encryption, Mobile forensic, Private chat.

1. INTRODUCTION

Specifically, from the private chat applications point of view, many applications are secure or claim to be secure due to the utilization of an encryption mechanism

* **Corresponding author Hepi Suthar:** Rashtriya Raksha University, Gandhinagar, India and Vishwakarma University, Pune, India; E-mail: hepisuthar@gmail.com

[1]. This is great because who does not want robust security around the aspect of privacy? However, this article intends to show how certain data can still be recovered despite encrypted databases that can certainly bring some information.

Forensic value is opposed to having absolutely no data. The main aim is to also stress the point that just because the main databases, which store all the crown jewels, are encrypted, does not mean you do not go through the rest of the data to find something of relevance if such data exists [2]. Since then, many versions of Dust, along with software updates related to iOS, and different Apple devices have been released [3]. Has anything changed since Heather's discovery? In the quest to address this question, we then started utilizing Joshua Hickman's iOS 14.3 test image [4, 5] to parse the populated data associated with Dust because, during the research, no one came across any post about forensic extraction from Dust v7.0.31183 RC running on an Apple device with the 14.3 software update. Here, consider the dust chat application [6, 7]. Fig. (**1**) describes the working method of end-to-end chat application architecture.

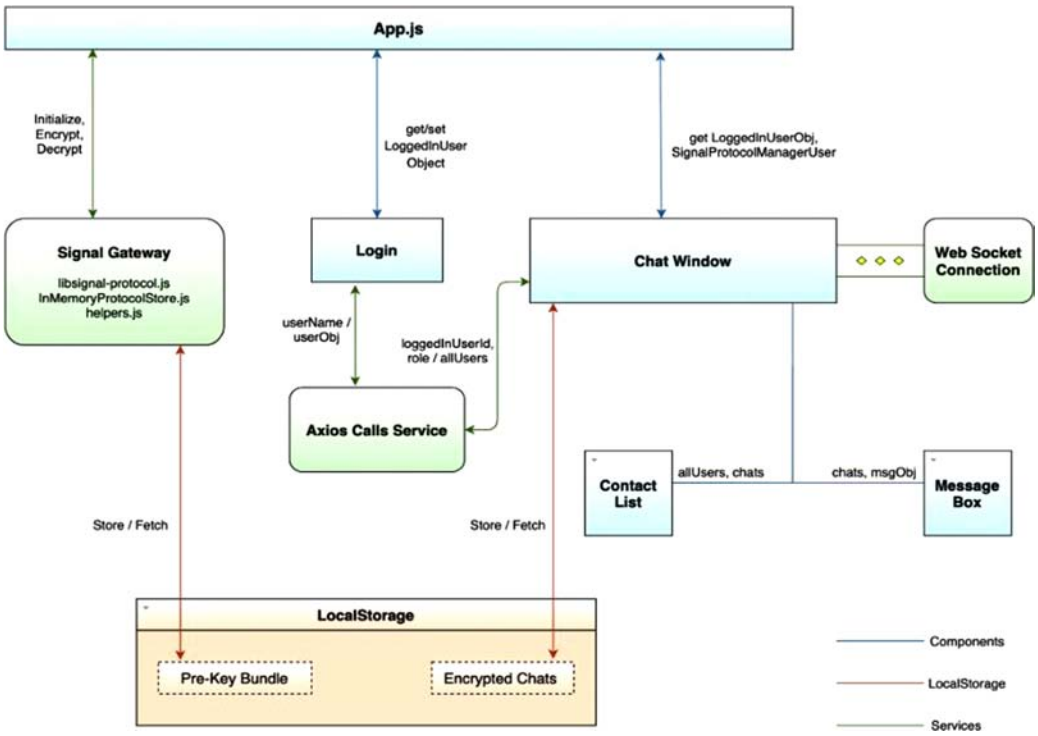


Fig. (1). End to End chat application structure [8].

2. EXPERIMENT WORK

During this testing, we solely utilized Autopsy v4.19.2, Hex Editor Pro v6.54, and MongoDB Realm Studio v11.1.1. The data populated by Joshua Hickman related to Dust is shown below in Table **1**. As stated earlier, it populated this data on an iPhone SE running iOS v14.3 and Dust application version 7.0.31183 RC. Again, the goal is to find anything apart from data that we expect to be encrypted as Dust claims [9].

Table 1. Dust Application Data Population by Joshua Hickman.

Name	**Dust**	-	
Version Number	**7.0.3.1183 RC**		
Install Date	**2021-01-30**		
Install Time	**10:53**		
User Name	**Thisisdfir100**		
Date	**Time**	**Action**	**Message**
2021-02-02	13:43	Login to app	
2021-02-19	15:32	Sent message	Man, I got tired of Firefox Focus and Onion Browser real quick.
-	15:33	Received message	Onion Browser is really slow.
-	15:34	Sent message	I know. The proxies. And it gets blocked on some websites.
-	15:35	Received message	Really?
-	15:36	Sent message	Yes. Cloudflare blocked me on Cult of Mac.
-	15:37	Received message	Wow. Some really don't want to get spammed, do they.
-	15:38	Sent message	No, and I can't blame them.
-	-	Received message	Here comes a picture.
-	15:39	Received picture	*(4 Chrome Tabs)*
-	15:40	Sent picture	*(Summertime Car Play)*

Below are the findings: First, the forensic image is downloaded, "iOS 14–3—Apple iPhone SE.tar," and extracted so it could be processed further as a logical folder into Autopsy for parsing, as shown in Fig. (**2**) below:

Below is the display of the file system folders associated with this image shown in Fig. (**3**).

CHAPTER 4

Browser Analysis and Exploitation

Tripti Misra[1,*], Devakrishna C. Nair[1], Prabhu Manikandan V[1] and **Abhishek K. Pradhan[1]**

[1] *School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India*

Abstract: Browsers are utilized in one form or another to browse the internet since they have become an essential component of our online lives. Additionally, we may use browsers to navigate the OS's file system in addition to using them for web browsing. It has been noticed that by default, browsers save data including credit card numbers, usernames, passwords, form data, emails, and other sensitive information. Additionally, downloaded media including images, videos, executables, documents, *etc.* are present in browsers. A user's browsing habits and interests can be inferred from their bookmarks and browsing history. Thus, browsers keep a lot of private data about users and their browsing patterns. Due to the type and volume of data they store with them, they play a crucial role in forensics. Depending on the platform being used, there are a variety of web browsers accessible, including Safari, Chrome, Firefox, IE, and Opera. This chapter will teach us how to do forensics on various types of browsers. The following are some of the numerous places an investigator could look for evidence online like Bookmarks, Downloads, Cache, Cookies by surfing history, and many more. This chapter also discusses browser exploitation and issues involved in forensic investigation.

Keywords: Browser investigation, Browser exploitation, Computer forensics, Chromium vrowsers, Web browser forensics.

1. INTRODUCTION

Internet users are growing daily, therefore evidence relating to browsers can provide light on critical aspects of cybercrime. With such widespread use of prominent social networking websites and online services for banking, shopping, *etc.*, the likelihood of potential cybercrimes is on the surmountable rise. Therefore, in a cybercrime investigation, the requirement for gathering Internet browsing-related data *via* a Browser Forensics Analysis is inevitable. By examining browser-related files on the hard drive that contain cookies, cache, and

[*] **Corresponding author Tripti Misra:** School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India; E-mail: tripti.misra24@gmail.com

Akashdeep Bhardwaj & Keshav Kaushik (Eds.)

other historical data, browser forensics may be performed as part of offline forensics. However, the amount of information that these files typically hold varies depending on the user's preferences. However, when a live forensics strategy is used, physical memory serves as the main repository of data that is pertinent to a given case. As a result, there is a very high likelihood that critical information might be gleaned from the suspect's computer by evaluating physical memory material that has been acquired. This article [1] describes a method for collecting user credentials from popular Web apps by looking at the physical memory data of a Windows machine. It aids cybercrime detectives in locating usernames and related passwords used in a variety of online mail accounts, online banking, and retail sites, among other things. The extraction of highly relevant browser forensics data pertaining to the suspect's Internet behaviour *via* memory dump analysis is another crucial approach the report discusses.

One may extract sensitive information and select keywords from most online browsers with the use of forensics tools like browser forensics. One can retrieve deleted data and keywords, confirm that the history has been erased, and retrieve artefacts such as cookies, download history, history, and passwords that have been saved, websites visited, *etc.* Additionally, Browser Forensics is extremely helpful in figuring out how an attack on a system was carried out, assisting in identifying the origin of Malware/Adware/Spyware, Malicious Emails, Phishing Websites, *etc.*

Browser forensics [2] is mostly used to examine a computer's browser history and general web activity in order to look for any suspicious behaviour or content access. In order to obtain accurate information about the targeted system, this also relates to tracking website traffic and analysing server-generated log files. The goal of computer forensics, a type of forensic investigation, is to characterise and analyse the digital evidence that is stored on computers and related storage media.

Nearly everyone, even suspects under investigation, uses the internet. A suspect could use a web browser to gather information, mask their crime, or look for new ways to commit crimes. A key aspect of digital forensic investigations is often searching for online browsing-related data. Thus, almost every action a suspect took while using a web browser would be recorded on a computer. This data can thus be helpful when a detective examines the suspect's computer. It is possible to examine evidence from a suspect's computer, including cookies, cache, history, and download lists, to determine the websites visited, when and how often they were accessed, and the search terms the suspect used.

2. LITERATURE REVIEW

In incident response, browser forensics plays a significant role in determining the origin of a breach and the origin of an attack on a machine or computer network. Given that more criminal and civil cases may be founded on evidence gathered from user online activity, web browser forensics plays a significant role within computer forensics. Investigators and criminals both utilize the internet. Criminals utilize web browsers to gather information for new criminal tactics or to hide their crimes. Criminals leave traces on computers every time they use a web browser. The cache, temporary files, index.dat, download files, cookies, browser history, and other data can all be used as evidence. In this research [3], the main online browser analysis tools have been discussed along with their advantages and disadvantages.

The procedure of gathering forensically reliable evidence from an active computer system is known as live forensics [4]. Live forensics are crucial in cyber forensics and must be carried out in order to gather volatile data. Live forensics are performed while the computer is active at the crime scene since once the machine is turned off, the information is permanently lost. Additionally, this method is favoured for forensically examining dedicated mission-critical servers. It is important to make sure that only pertinent data is taken from the suspect's hard drive during live forensics. This is done to lessen the amount of tampering with the original evidence.

Because browser files hold crucial information about a suspect's online activity, both offline and live forensic investigations depend heavily on their examination. In this article, a framework that can acquire and analyse browser files is explained [5]. The framework's acquisition tool has the ability to forensically recover the suspect's computer's browser files. The analysis programme examines the downloaded browser files to discover forensically important data about Internet Activities. In the study, browser forensics of popular web browsers is detailed. The detectives can get important clues about the crime using this approach. This might support the argument that the suspect's computer was where the alleged cybercrime-related Internet activity took place.

A subfield of forensic science is digital forensics. Internet users are currently growing daily, and as a result, online crimes are rising. Digital forensics involves utilising digital devices to retrieve information and determine if they have ever been seen or hacked. Digital forensics' main goal is to collect the “evidence” from crime scenes. An extension of computer forensics, digital forensics encompasses digital electrical devices like printers and cell phones. Because more criminal and civil lawsuits may be founded on evidence gathered from user online activity, web

CHAPTER 5

Data Recovery from Water-damaged Android Phones

Ankit Vishnoi[1,*] and **Varun Sapra**[2]

[1] *School of Computer Science and Engineering, Manipal University Jaipur, India*

[2] *School of Computer Science, University of Petroleum and Energy Studies Gurugram, India*

Abstract: Mobile phones can occasionally be damaged by water, but forensics professionals can frequently still recover the evidence. The efficacy of various forensic techniques has been examined in this chapter. We use hardware and software tools to gain direct access to the phone's memory chips since a damaged phone might not be powered on and the data port might not function. These include hacking instruments, the ones that may be used to retrieve data from mobile devices. The chapter discusses strategies that apply to Android mobile devices. Additionally, the study only explored techniques for accessing data—not for decrypting it. Mobile devices can sustain water damage as a result of inadvertent exposure to water or deliberate attempts to remove forensic evidence. Traditionally, chip-off analysis has been chosen as a successful data recovery technique for damaged devices, particularly those that have been water-damaged. In this essay, we investigate what transpires inside portable electronics when they are submerged in water. The likelihood of successfully conducting forensic data recovery on a water-damaged mobile device is high if the right steps are taken and the relevant processes are followed. This chapter discusses common water damage diagnoses as well as efficient restoration techniques.

Keywords: Android data recovery, Mobile Forensics, Mobile data acquisition, Smartphones, Water damaged mobile.

1. INTRODUCTION

Before starting to use the recovery techniques, one needs to make sure that your phone has been through water damage. This will make it easier for you to retrieve files from a phone that has been dropped into the water, by following the right procedures. However, the few signs that are listed below will enable you to recognize that your Android phone has water damage. Anything that comes in contact with water fully shuts down, and Android devices are no exception. If

[*] **Corresponding author Ankit Vishnoi:** School of Computer Science and Engineering, Manipal University Jaipur, India; E-mail: avishnoi@ddn.upes.ac.in

Akashdeep Bhardwaj & Keshav Kaushik (Eds.)

placed into liquid, it ceases to function. Android customers report that when their phone goes into the water, it feels as though the entire world has frozen. If you have a waterproof smartphone, you can get around this. In general, Android devices have gained a lot of popularity in the previous few years because of their amazing and distinctive features. Smartphones have an advantage over other phones because of these qualities.

However, it is not yet over. Due to these factors, smartphone manufacturers are now creating waterproof models so that customers won't experience any form of data loss issue. Indeed, most individuals today don't have waterproof smartphones, which necessitates the use of alternative solutions to deal with the matter. Every Android user should be aware that taking care is one of the most important things they can do to keep their phones from getting wet. But what should you do if it's already too late and your phone has fallen into the water? Here are some crucial details about water-damaged Android phones and ways for data recovery from water-damaged phones.

1.1. Phone Parts Damaged when dropped into the Water

With a nice smartphone or not, one thing is certain: if your phone falls into the water, it won't know how to swim. Some crucial components of Android phones are harmed when they come into contact with water. However, a lot of consumers are unaware of what the damaged portions are.

The phone has a single motherboard, which is made up of crucial parts including the RAM, CPU, and other little pieces. The headphone jack, microphone jack, and charging port are three of the most common places where water enters an Android cellphone while it is wet. The motherboard and phone screen are both damaged as a result. After that, the expensive machine is used as a kid's toy. Once the equipment has water damage, it is hard to restore the same level of feel and touch. And if a lot of effort is put into bringing the item to life, it will cost close to what the phone originally cost.

Liquid Damage Indicators, or LDIs, are typically included inside cell phones and cause the color of the device to change when it becomes wet. Some smartphones, including the Samsung Galaxy, have this functionality where the battery is represented by a white sticker with red-covered little Xs. This sticker changes color when it is wet, turning purple, red, or pink. And only when the battery is wet with water or another liquid does this occur. Figs. (**1** and **2**) show normal batteries and water-damaged batteries [23].

Fig. (1). Normal mobile Battery [23].

Fig. (2). Water-damaged battery [23].

1.2. What Should One Do If the Phone Gets Wet or Contacts Any Liquid?

The Android device has experienced many issues when dropped into the water. This is due to the device's storage of several necessary items and, more importantly, the fact that it is not waterproof. However, some steps that can be used to resolve the issue are described here. Assume your Android device accidentally falls into the water as shown in Fig. (**3**). What should you do?

CHAPTER 6

Machine Learning Approach to Detect Ransomware Threats in Health Care Systems

Varun Sapra[1,*], **Ankit Vishnoi**[2] and **Luxmi Sapra**[3]

[1] *School of Computer Science, University of Petroleum and Energy Studies Gurugram, India*

[2] *School of Computer Science and Engineering, Manipal University, Jaipur, India*

[3] *School of Computing, Graphic Era Hill University, Dehradun, India*

Abstract: With the advancement in healthcare technology, the industry is moving from conventional diagnosis methods to digital health platforms. These digital health platforms are useful for patients in different ways like from initial disease diagnosis to drug prescription and maintaining electronic health records. These health records contain a lot of personal information of patients that has high monetary and intelligence value, so such healthcare systems are more vulnerable and targeted by cyber thieves. Several techniques have been implemented by healthcare organizations for the early detection of such cyber threats and for securing the medical records of patients. One such method is machine learning (ML) for the detection of threats or adulterated data due to some payload ransomware. This chapter highlights different healthcare data breaches and the impact of cyber-attacks on medical data using artificial neural networks.

Keywords: Artificial neural network, Cyberattacks, Electronic health records, Healthcare system, IoMT.

1. INTRODUCTION

In the past decade, with the progression in technology, especially in the area of information services, the health sector has been transforming at a rapid pace and producing a large amount of medical information. There are lots of reasons for the information outburst. The palpable one is the increase in technology. As the potential of digital procedures increases and prices plummet, every business is using more and more technology to automate processes and to get real-time data for business decisions. Healthcare also has not been left out of this. This medical information contains a huge amount of complex medical data about patients including inter alia, clinical parameters, hospital resources, medical devices,

* **Corresponding author Varun Sapra:** School of Computer Science, University of Petroleum and Energy Studies Gurugram, India; E-mail: varun.sapra@gmail.com

Akashdeep Bhardwaj & Keshav Kaushik (Eds.)

disease diagnosis, and patients' records [1]. Such data has high intelligence and monetary value for cyber attackers. As per the 2021 H2 healthcare, data breach report cybersecurity breaches hit an all-time high in 2021. 34 million people were affected due to such healthcare data breaches in 2020 whereas the number reached 45 million in 2021 for such affected patients [2]. Fig. (**1**) shows the no. of healthcare data breaches from the year 2009 to 2021 [3].

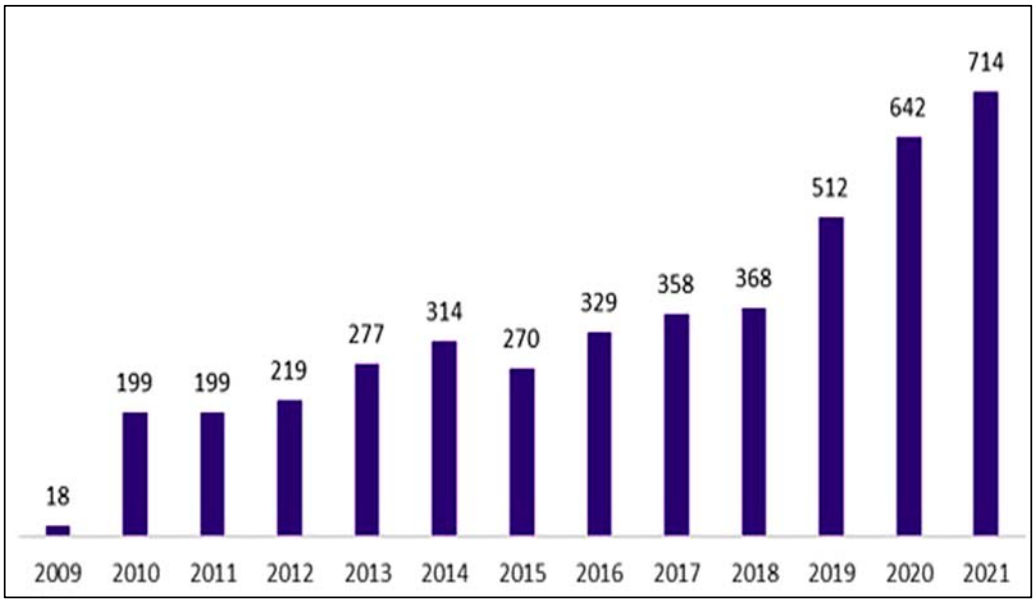


Fig. (1). Healthcare Data Breaches from 2009 to 2021 [3].

Although the number of data breaches is maximum in 2021, the no. of patient records exposed was maximum in 2015. Around 113.27 million records were exposed due to three massive data breaches. Fig. (**2**) shows the number of records exposed each year from 2009 to 2021.

Another way to impact healthcare records is ransomware attacks. Ransomware is a type of malware that is used to encrypt the data partially or completely and make it unusable for the system to work. Ransomware can be categorized as crypto and locker. Crypto-ransomware works on encryption and is used to encrypt user files on a computer. Cybercriminals then force the user to pay the ransom for accessing their files. In the case of locker ransomware instead of encrypting the user files, it locks the system and restricts the user to log in, making it inoperable.

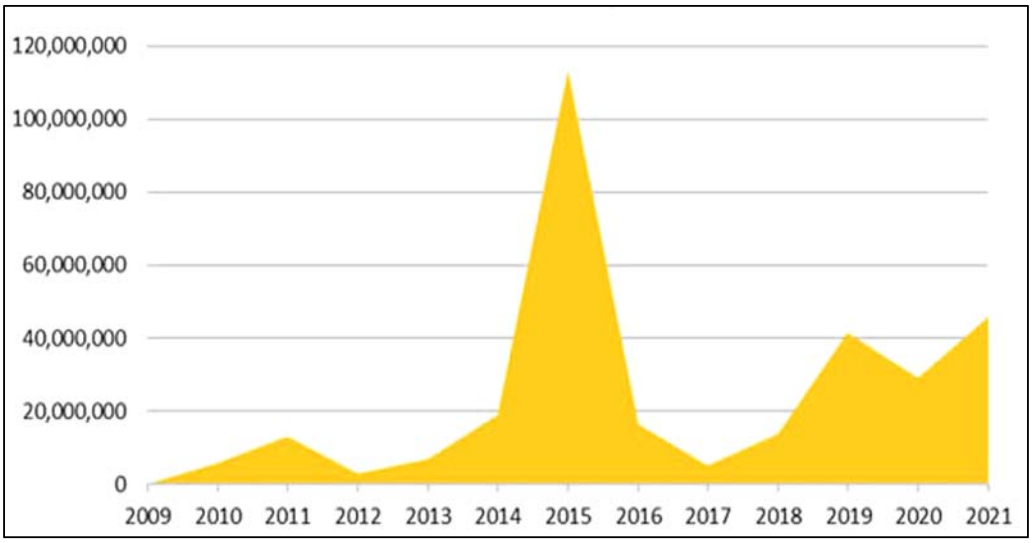


Fig. (2). No. of patient records exposed in data breaches [3].

During the pandemic, hospitals were at the maximum risk of ransomware attacks. In 2020 and 2021, there were around 168 ransomware attacks that affected 1763 health centers in the US only [4]. Hospitals are prime targets for ransomware because of three major factors: money, the criticality of the data, and access points. Some of the major ransomware attacks that happened from 2015 to 2021 are shown in Table **1**.

Table 1. Major Ransomware attacks from 2015 to 2021 [5].

S. No	Organization / Company	Date	Impact
1	Kaseya (IT Solution Providers)	July 2, 2021	Approx. 1500 organizations in multiple countries.
2	JBS (largest Meat Suppliers)	May 31, 2021	The company has to stop its operations in five US-based plants.
3	Colonial Pipeline (refined Products)	May 7, 2021	Gas price per gallon increased to 43 in the US in seven years.
4	Brenntag (German chemical distributor)	April 28, 2021	The company paid $4.4 million.
5	CNA Financial (Commercial Insurer)	March 23, 2021	A major part of the data was hacked.
6	CWT (Business Travel Management Firm)	July 31, 2020	Infected around 30,000 computers and steal sensitive files.

SUBJECT INDEX

A

B

C

D

E

F

H

I

L

M

N

P

Q

R

S

T

W

Akashdeep Bhardwaj

Prof. Akashdeep Bhardwaj is working as professor (Cybersecurity & Digital Forensics) at the University of Petroleum & Energy Studies (UPES), Dehradun, India. Prof. Akashdeep has worked as a technology leader and head of several multinational organizations. He is an eminent IT Industry & Academic expert with over 27 years of experience in cybersecurity, digital forensics, and IT management operations. He is the mentor of graduate, master's, and doctoral students from national and international universities apart from leading cybersecurity projects. He has published over 100 research papers in SCI/WoS/Scopus journals, several books & chapters, and four patents.

Keshav Kaushik

Keshav Kaushik is an experienced educator with around ten years of teaching and research experience in cybersecurity, digital forensics, and the Internet of Things. He works as an Assistant Professor (Senior Scale) in the systemic cluster under the School of Computer Science at the University of Petroleum and Energy Studies, Dehradun, India. He has published over 100 research papers in international journals and has presented at reputed international conferences. He holds certifications including Certified Ethical Hacker (CEH) v11, CQI and IRCA Certified ISO/IEC 27001:2013 Lead Auditor, Quick Heal Academy Certified Cyber Security Professional (QCSP), and IBM Cybersecurity Analyst. He has delivered over 50 professional talks as a keynote speaker on various national and international platforms. Additionally, he has edited more than twenty books with esteemed international publishers such as Springer, Taylor and Francis, IGI Global, and Bentham Science. He has chaired various special sessions at international conferences and served as a reviewer for peer-reviewed journals and conferences. Currently, he serves as the Vice Chairperson of the Meerut ACM Professional Chapter and is a brand ambassador for Bentham Science. Moreover, he is a guest editor for the IEEE Journal of Biomedical and Health Informatics (J-BHI) (IF: 7.7).