An Exploration Analysis of Social Media Security

Shreeja Verma and Sushruta Mishra

Abstract Social media security is a rising concern among today's generation, as when the pandemic started, a lot more people than before have begun using social media due to lack of entertainment or other reasons. There is a rise of 62% in Ransomware since 2019 (pre-pandemic), as mentioned by the Cyber Threat Report by SonicWall. As cybersecurity attacks are becoming more severe, this number of attacks is still set to rise. So in order to investigate the possible security issues, this paper digs deep into the concepts of social media security, potential threats and feasible solutions. The importance of having users' data secure and protected from various threats such as malware attacks, identity theft, cyberbullying and so on, is addressed so that neither the user nor the developers suffer from any loss. Organizations may do more effective patch management to prioritize security-related patching and update their software in accordance with the solutions discussed in this paper.

Keywords Exploits · Vulnerabilities · Malware · Steganography · Metadata · Third-party

1 Introduction to Social Media Security and Its Evolution

As we have stepped into the second decade of the twenty-first century, we have seen technology grow remarkably in comparison to the times when smartphones were non-existent. With the advent of social media platforms like WhatsApp, Facebook, Instagram and Twitter, we have not only witnessed the creation of a new standard of communication but also an increase in security issues despite the various efforts made by the developers of these platforms [1].

In the early 2000s, with the advent of social media, cybercrime began to take its toll. The influx of personal information into profile folders has led to the emergence of ID fraud. People with malicious intent use information to set up bank accounts, suspend credit cards or engage in other forms of financial fraud in various ways.

S. Verma · S. Mishra (✉)
Kalinga Institute of Industrial Technology, Deemed to Be University, Bhubaneswar, Odisha, India
e-mail: sushruta.mishrafcs@kiit.ac.in

H. K. Thakkar et al. (eds.), *Predictive Data Security using AI*, Studies in Computational Intelligence 1065, https://doi.org/10.1007/978-981-19-6290-5_2

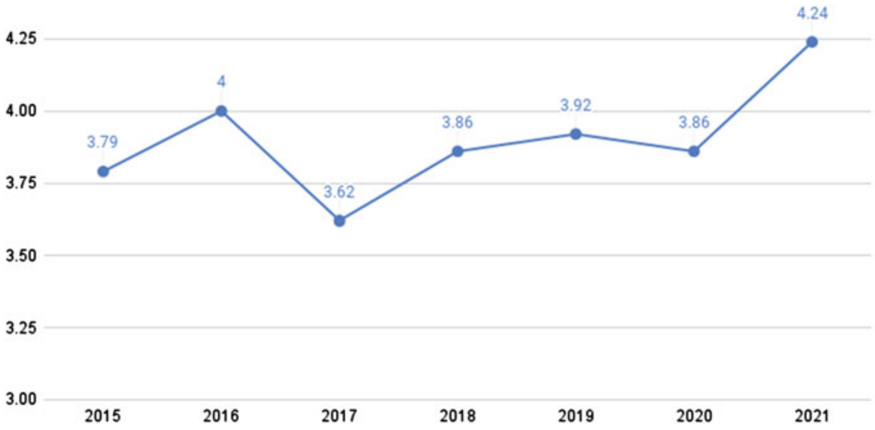

Fig. 1 Average total cost of a data breach (in US$ millions)

Currently, ransomware threats are increasing because criminals are pursuing threats to disclose information they have gained through the social media profile of an individual or organization. Ransomware is a type of malware program that limits users and system administrators' access to files or all networks. If a malware program invades systems, attackers will send a ransom note usually authorizing payment via Bitcoin. Ransomware made history in 2020 contributing to the first reported deaths related to cyberattacks. In this case, the German hospital was closed off from its programs and could not treat patients. A woman who needed urgent care was taken to a nearby hospital 20 miles away but did not survive. According to the report rendered by IBM, In 2021, inflation in the average total cost of a data breach was the highest amount in 7 years [2]. Data breach costs have increased considerably between the years 2020 and 2021, growing from $3.86 million in 2020 to $4.24 million in 2021 (Fig. 1).

With such extreme threats and vulnerabilities, social media cybersecurity comes into action. For the users to be able to rely on these social media platforms, it is necessary to constantly monitor the security threats and vulnerabilities and fix them as soon as possible. It is also important to be able to detect such threats in advance before it comes to the notice of a pernicious client who later exploits these vulnerabilities [3].

2 Important Issues Involving Security for Social Media

While millions of users share their content on social media without any worry for their data, there exist issues that concern the security of these vulnerable platforms that are prone to be exploited by hackers. Some extremely important ones associated with it are listed below.

2.1 *Privacy of Data*

When users share their personal information on social media, there are many ways in which this data can be misused by corrupt clients around the world [4].

2.1.1 Metadata

Social media content has a lot of metadata, which can be used by cyberstalkers to gather information about their targets. For instance, if they have access to a person's location, they can easily find out their device's details. In our day-to-day lives, we come across metadata more frequently than we know. Each time you open an e-mail, read a book or order something off Amazon, or while communicating over the telephone, you've come upon metadata (Fig. 2).

Law enforcement organizations around the globe are infamous for using metadata from e-mails, digital messages and other forms of telecommunications to conduct investigations and achieve their goals. In 2015, when the Australian Parliament made it obligatory for communication carriers to keep a 2-year database of all telephone metadata, a media storm erupted as critics considered the site a hacker's honeypot, claiming that data theft could lead to serious damage to citizens' privacy [5].

2.1.2 Shared Ownership

In the age of sharing a humongous amount of data with each other, where just a single client can manipulate the protection settings of the particular multimedia, often results in proprietorship loss on the content. For example, you may have access

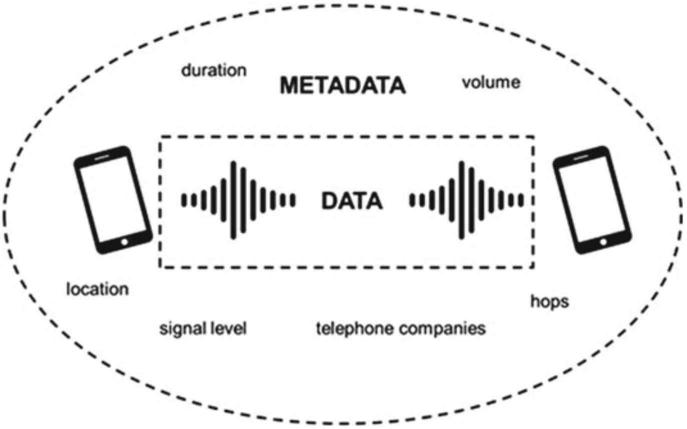

Fig. 2 Example of metadata [36]

to edit a google document but someday due to personal grievances, the creator might change the access settings to private, resulting in loss of ownership of the document.

2.1.3 Tagging

While posting multimedia content, a user not only puts his/her personal information at risk but also puts the ones, who are not active users or may not be a user of the particular platform at all, in danger as well by revealing personal information about more than one user, by tagging others in a single post [6].

2.1.4 Social Engineering

Undermining the security of sensitive data of an organization to acquire it for malicious activities is called Social Engineering which happens due to the exploitation of personal trust. Social networking sites, such as [7] Facebook, allow you to create your own page and interact with a network of people who may contain malicious users. By exploiting the trust the user has in his or her network, cybercriminals can embed malware or computer viruses on the content of their Facebook friends which can further lead to more users being duped.

2.2 Data Mining

We all leave our digital footprint anytime we interact with the internet [8]. At any point in time, if we create a social media account, we leave behind a set of traceable digital activities, actions, contributions and information. This data trail can be stored in various ways and can be exploited by attackers.

2.2.1 Third-Party Access

Users may delete or deactivate their social media accounts, but they may not be able to erase the data that the platform has shared with the third-party vendors, who are usually in a high-risk area for privacy breaches. Targeted advertising, which is another byproduct of all the data provided to the third-party platforms, may collect our real-time information without our knowledge.

According to a blog post by Yaffa Klugerman (Director at Panorays), listed below are the Five Most Noteworthy Third-Party Data Breaches in the year 2021:

1. **Accellion**: Late last year, the vulnerabilities in Accellion's File Transfer Appliance were used by cybercriminals [9]. The Accellion's File Transfer Appliance is used for the mobility of large and crucial files inside a network. Their victims

included the State Bank of New Zealand, Washington State, Kroger Grocery Store, the University of Colorado, cybersecurity company Qualys and many others.

2. **Audi and Volkswagen**: Earlier in the year, the Volkswagen Group of America, Inc. came to know about the insecure data that was dumped on the internet by one of its sellers, which was acquired by some illegitimate group. The violation hit 3.3 million consumers, which is more than 97% of Audi customers and interested consumers [10–12].
3. **Click Studios**: In April, Click Studios informed its customers that a business password manager, Passwordstate, a business password manager, was hacked by cybercriminals who exploited Click Studios' update system and delivered malware to customers. Click Studios notified its users about this in April as it had affected more than 370,000 security and IT professionals in 29,000 companies globally.
4. **Cancer Centers of Southwest Oklahoma**: An unauthorized access to protected data which included names, Social Security numbers, addresses, treatments and medical diagnoses, for around 8000 oncology patients was made in 2021. The cloud-based storage provider for the Cancer Centers of Southwest Oklahoma, Elekta, received an unusual outburst on their network which lead to this breach.
5. **Kaseya**: There exist many groups of malevolent attackers infamous for their malicious intent, one of them, known as REvil ransomware team, attacked Kaseya VSA, which is a remote monitoring and management software platform. Kaseya had to close down both the on-prem and the SaaS servers as a precautionary measure after that, as about 1500 companies were hit worldwide [13].

2.2.2 Profiling and Profile Cloning

Clients with malicious intent may often keep a close watch on their target's social media account to extract every bit of information from the content they post. Thorough data analysis can further help the attackers in profiling and profile cloning, which can lead to blackmailing, cyberbullying and cyberstalking.

2.2.3 Corporate Espionage

Big organizations using social media accounts for marketing purposes may help attackers to assemble internal data through the content that is being posted. Competing companies might use this information to destroy the reputation of the concerned organization and hence encourage such spies to keep a close eye on every bit of information [14–16].

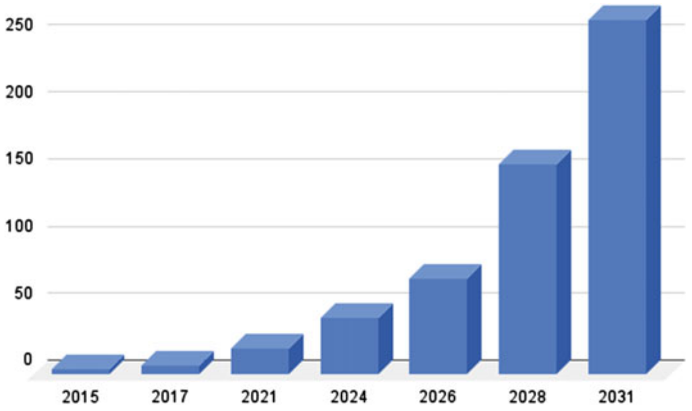

Fig. 3 Global ransomware damage cost prediction (in billion USD)

2.3 Virus and Malware Attacks

2.3.1 Malware Attacks

Attackers often use malevolent URLs to direct users to a site that installs malware in their systems. These further help the attackers in extracting confidential data from the user's PC such as passwords and account details. Cybersecurity Ventures revealed in an article that by 2031, ransomware will probably take a toll on its targets by costing them more than $ 265 billion (USD) annually, with new entries every 2 s as ransomware hackers gradually improve their loading of malicious software once and for all, and related fraudulent activities [17]. The dollar figure is based on a 30% annual growth rate in damages over the next 10 years (Fig. 3).

2.3.2 Phishing

Phishing, a word derived from the word fishing which means 'baiting' people [18], is generally done via emails or texting. It guides the user to a fraudulent website and asks for private information such as usernames and passwords of bank accounts or other official accounts. 2021 Tessian research has revealed that employees get an average of 14 malevolent emails per year. A few industries were affected worse than the others, with retail workers receiving an average of 49. Mishra et al. [19] CISCO's 2021 report on cybersecurity threats shows that at least one person has clicked on a link to a phishing website at about 86% of organizations. Company data suggests that phishing accounts for about 90% of data breaches. CISCO also found that phishing is often high during the holidays, based on the fact that the number of phishing attacks increased by 52% in December.

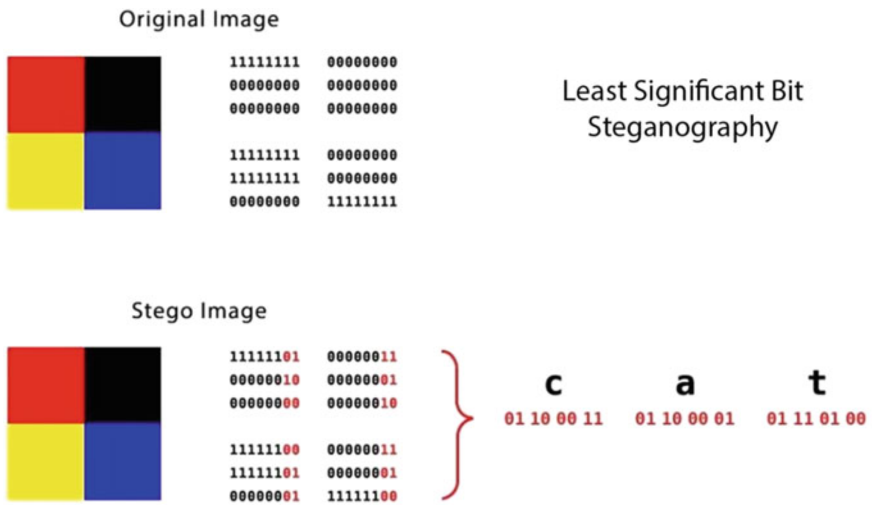

Fig. 4 Example of steganography—least bit steganography [37]

2.3.3 Steganography

The practice of concealing information in different objects has been observed for ages. Before the computer was built, sensitive messages were hidden in furniture, quilts, paintings and so on. But in today's time of technological advancements, attackers are using digital media to conceal malicious data in plain sight. For instance, an image of a dog may contain some malevolent code that gets triggered once clicked and it deletes all the system files from your computer. Using images to conceal data is the most common form of steganography in today's time and attackers may change just the least significant bit that does not affect the appearance of the image and is not detectable by the naked eye (Fig. 4).

It is important to note that Cryptography and Steganography are not alike and they have complementary purposes. Information might be encrypted and then concealed using Steganography.

2.3.4 Click-Jacking

It is an attack that lets a user click on a web page element that is hidden or corrupted with a malicious element that can lead to unwillingly installation of malware, transfer money or submit important usernames and passwords [20].

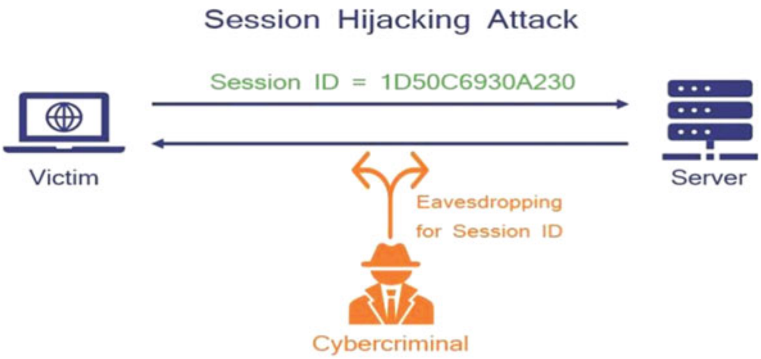

Fig. 5 Session Hijacking attack [38]

2.3.5 Session Hijacking

A type of man-in-the-middle attack used to exploit social media accounts. It occurs when an attacker steals a session cookie, which can provide identity, access and tracking information when active. It can also occur when the attacker injects malicious code into frequently used websites by its target (Fig. 5).

According to Alabrah et al. [21], there are three types of Session Hijacking:

1. Active Session Hijacking—Attacker attacks on an already operational session between user and server. The attacker puts himself in the position of a legitimate user with a DOS attack.
2. Passive Session Hijacking—Here, the attacker positions himself in the middle of the legitimate user and the server. He receives the packet in between the transition of the packet from the user to the server. The attacker can also alter the information carried by the packet to achieve his mischievous goals. The only disadvantage for the attacker here is that he can have access to the packets only till the session is active [22].
3. Hybrid Session Hijacking—It is a combination of both active session and passive session hijacking. It can further be divided into categories: Blind Spoofing Attack and Non-Blinding Spoofing Attack [23].

2.4 Legal Issues

2.4.1 Grooming

When an adult (18 years or above) makes an attempt to trap minors through the internet (games or social media platforms) with the intent of sexual assault, it is called grooming [24]. Social media opens the door for such paedophiles, as they can easily communicate with their targets. They may impersonate someone else or try to befriend them through their jovial act.

Table 1 Data breaches in well-known digital platforms

Organization	Year	Impact
Aadhaar	2018	1.1 billion people
LinkedIn	2021	700 million users
Facebook	2021	533 million users
Twitch	2021	700 million users
Twitter	2018	330 million users
Dubsmash	2018	162 million users
MeetMindful	2021	2.28 million users
Raychat	2021	150 million users
Tinder	2020	70 thousand female users
TikTok	2020	235 million accounts
Instagram	2019	49 million records

2.4.2 Cyber Bullying

With more and more young teenagers joining social media platforms, there has been a drop in social media security. There have been many instances where media content of young girls has been manipulated and exploited on social media by pernicious clients [25].

3 Risks and Challenges of Social Media Security

3.1 Information Revelation

The term 'data spill', according to the National Security Agency, refers to the transfer of isolated or sensitive information to unauthorized systems, people, applications or media. A multimedia substance with its metadata when uploaded on social media platforms, or Data breaches at third-party apps lead to the revelation of personal and confidential information to the attackers. Malware that gets installed on a user's PC through a malevolent URL might extract all the personal data stored on the system, hence leading to Data Disclosure [26] (Table 1).

3.2 Location Spillage

Third-party apps that have access to the user's real-time data, data breaches, metadata and multimedia content exposure on social networking sites often result in the leak of the location of the user [27].

3.3 Cyberbullying and Cyberstalking

With the increasing ease of communicating with people around the globe, there has also been an upsurge in cyberbullying. A user can interact with his/her friends or even with celebrities through public comments on their posts. Many users use this as a medium to pass lewd comments, spread rumours and hatred around them. Hackers easily get access to a user's account and their data, after which they may misuse it or even blackmail the user [28].

3.4 Cyber Terrorism

The nature of terrorism threats has considerably changed over the past 20 years. Social media has now also become a medium for terrorists to spread hatred and rumours around society and hence convince a larger group of people to support their inhumane cause. In 2017, organizations in more than 150 countries were struck by the two highly vicious attacks of WannaCry and NotPetya, that caused losses estimated at more than USD 300 million along with the damage to reputation because of the loss of customer data. And as the cyberattackers get more and more adapted to the older security barriers of the social media accounts, we can now also observe the shift in the nature of cyberattacks; from individual consumers to global political and economical systems.

3.5 Reputation Misfortune

Often corporate employees, school students or social specialists who have the agenda of degrading a superior's reputation, make use of social media platforms. These lead to the downfall of a person's or an organization's prestige.

3.6 Identity Theft

Social media platforms like Facebook or Instagram have billions of users who have stored their personal information or constantly post tremendous amounts of content that increases the risk of leaking personal information has become a hub for attackers to utilize this data to apply for loans or commit other financial fraud without being caught.

4 Social Media Networks Security Solutions

Social media threats are more ostensible now than ever and thus, many researchers have developed various security measures to curb vulnerabilities and cybercrime [29].

4.1 *Watermarking*

Watermarking represents the commercial application of steganography and its potential aim is to reduce cybersecurity risks. It is the process of embedding a piece of code, sound or any tag to identify the proprietorship of the content in which it is implanted [30]. It can be robust, i.e. information can be restored after a dangerous or weak attack, where the information cannot be duplicated or verified after basic flag correction. There also exists semi-delicate watermarking which is half powerful as delicate watermarking.

Currently, watermarking is used for

- Copyright protection—preventing third parties from infringing on digital media ownership.
- Fingerprinting—to obtain information about a digital media receiver (owner) to track distributed media copies.
- Copy protection—to prohibit data copying devices from copying the digital media if it is copy-protected.
- Image verification—originality of the digital media is verified.

The basic idea of watermarking involves the addition of a watermark signal to the host data that will be marked in such a way that the mark is invisible and protected in the signal. Watermark can be partially or fully obtained only if the cryptographically secure key is available (Fig. 6).

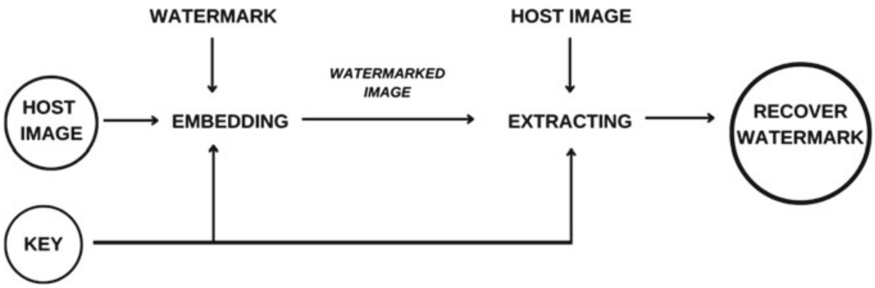

Fig. 6 Embedding and extracting process of digital marketing

4.2 Steganalysis

It is an approach to detect steganography by inquiring at differences between bit patterns and remarkably big files. The aim is to recognize suspected hidden data, find out whether or not they have got obscured messages encrypted in them and recover those messages if feasible. Steganalysis typically starts with numerous suspected information streams because of the uncertainty of whether these information streams incorporate a secret message. The steganalyst then begins by reducing the large set to a subset of most likely altered data streams. Analysis of encrypted information may also take several forms: obtaining, removing, disqualifying or demolishing encrypted information. The technique used in steganalysis relied on the information that can be gathered by the steganalyst, which includes only the steganography medium available for analysis, the hidden message known and so on [31]. In the procedure of steganalysis, the stego image is blocked and the steganalyzer also sometimes ties to extract the hidden message or information. Figure 7 shows the block diagram of the generic steganalysis process.

4.2.1 Steganalysis Techniques

Unusual Patterns

Suspicions for steganography arise from the detection of unusual patterns. There is a decline in the quality of digital media if it is being altered to conceal an object. For example in the case of Network Steganography, Packet headers are stuffed with strange patterns due to the fact that these packet headers are hardly read by anyone in general, thus making them a good hiding place [32].

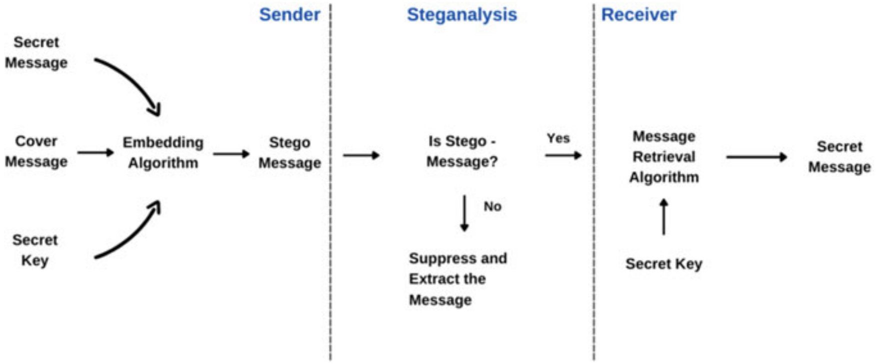

Fig. 7 Block diagram of steganalysis

Visual Detection

The identity of hidden data or a steganography tool can be detected with the help of analyzing repetitive patterns. Comparing the original image with a stego and thereafter observing noticeable differences is one of the methods to test these patterns. Such attacks where the carrier is known and discovered easily are called known-carrier attack. In case of unavailability of cover images, even the signatures that are received are enough to indicate the existence of a hidden message or to identify the tool that was used to embed these messages [33]. These hidden message signatures can be obtained by comparing multiple images. Other visible indicators of a hidden message include cropping or padding of images because a certain stego tool cuts blank spaces to fit a stego image into a fixed size. Other methods that can come under Visual Detection of Steganalysis Technique are noticing the variation in file sizes of the cover image and the stego image, or the differences in the colours of both the images.

Tools to Detect Steganography

Several tools to detect steganography are available, such as EnCase by Guidance Software Inc., ILook Investigator by Electronic Crimes Program, Washington DC, various MD5 hashing utilities, etc. An automated tool for detection, known as Stegdetect, provided by Niels Provos, is also quite popular. Stegdetect uses specific steganography-based applications, is used to find hidden data in JPEG images.

4.3 Digital Oblivion

Digital Oblivion is commonly known as the right to forget [34], meaning that data must be identifiable and usable for a limited time. This approach is very helpful in protecting the privacy of astronomical amounts of data since Online Social Networks are thriving with billions of users. Generally, there are two ways to implement digital oblivion using expiration dates, the first one relies on cryptography (such as employing expiration dates) and another in which the data is stored on an external, highly secured server [35]. Tools like X-Pire software creates encrypted copies of images and asks users to give each one expiration date.

But there are certain challenges that hinder the implementation of digital oblivion as pointed out in a recent EU report:

(i) allowing a person to locate where their data is stored,
(ii) tracking all the copies and the information deduced from the item,
(iii) to ascertain whether a person has the right to request for the removal of a data item and
(iv) affecting the erasure or removal of all exact or derived copies of the item in the case where an authorized person exercises the right.

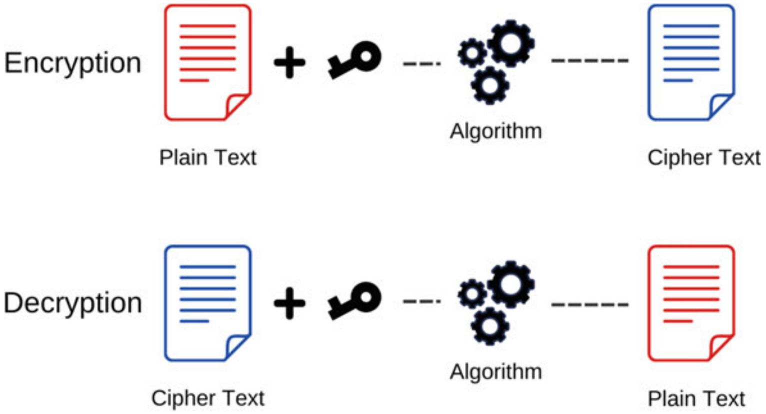

Fig. 8 Encryption and decryption of data

4.4 Storage Encryption

As many new social media platforms are emerging day by day, not each one of them owns private data centres. The majority of them store the user data on a third-party server. Personal user information may be shared with unauthorized groups by these third-party data centres for their own advantages and neglect the user's consent. So using encrypted storage and site encryption goes a long way in reducing the risk of data exploitation. In today's time, we use electronic tools to develop different data encryption algorithms to shuffle your data. Plain text or any type of data can be encoded using this methodology. The encrypted data can only be decoded by someone who has the decryption key to keep the data safeguarded. The encrypted data is generally referred to as ciphertext, while unencrypted data is called plain text (Fig. 8).

4.5 Detection of Malware and Phishing

Detection of Malware can be performed in multiple ways. Malware is a grave threat that leads to other serious problems such as ransomware and one may even remain unaware that their system has been infected by malware until it's too late.

4.5.1 Techniques for Malware Detection

Anomaly-Based Detection

There are two phases through which anomaly-based diagnosis can occur—the training (learning) phase and the adoption (monitoring) phase. During the progression of the learning phase, the detector tries to learn normal behaviour. The main advantage of anomaly-based discovery is its ability to detect zero-day attacks. The Zero-day attack as described is a previously unknown attack on the malware detector program. This process has two basic limitations: a high level of false alarms and complexity.

Static Anomaly-Based Detection

In statistical anomaly-based detection, specifications about the file system under review, are used to capture malicious code. The main advantage of statistical anomaly-based detection is that its use can make it possible to detect malicious software without allowing malware to run on the host system.

Hybrid Anomaly-Based Detection

(i) **Ghostbuster**: Wang et al. [7] suggest how to identify the type of malware that they call ‘ghostware’ by offering a ‘cross-view diff-based’ approach. Ghostware is a malicious computer program that can hide its presence in the operating system query programs. For example, all the resources of the ghostware will be invisible to a user if he/she executes a command to list files in the current directory, ‘dir.’

(ii) **Self–nonself**: The method proposed by Forrest et al. [8] is generally not accomplishable in real detection aids. The goal of the suggested method is to detect changes in protected data. The limit of this method is that it cannot detect the extraction of objects in a protected database.

4.5.2 Phishing

The majority of the strategies to detect phishing sites revolve around machine learning procedures in which highlights of sites are used in recognizing phishing websites. The phishAri process of ongoing ID theft crime that takes place on Twitter is a program that combines tweets posted with URLs into two categories: identity theft or authenticity using tweet’s objects. Another program, WarningBird, identifies malicious links posted via Twitter. They may be able to withstand the onslaught of identity theft by hiding malicious URL-based redirects.

4.6 Prediction of Cyberattacks Through Monitoring Social Media

Cybercriminals use socially explicit information to create exploit code as part of a series of cyber killing chains that follow a series of online attacks from the initial stages to data extraction. Social Media forums such as Twitter provide predictable details of potential zero-day attacks. This examination of potential pre-existing threats creates a time lag in the exploitation process; from the time, criminals receive information about the vulnerability, to the ultimate exploitation. It is found that using a monitored machine learning system such as Random Forest can help detect potential exploitation through the information available on Twitter (Fig. 9).

Sapienza et al. [13] developed a model that warns of the latest cyber dangers by constantly observing social media posts of highly qualified security researchers, analysts and dangerous criminals of white hats, posts related to attacks, threats and vulnerabilities. Sauerwein et al. [23] noted that there were discussions on about one-fourth of the perceived vulnerabilities on Twitter before they were disclosed in public and that Twitter could provide an opportunity to respond to newly identified risks, thus being a good source for preventing exploitation, crippling cyber crimes and benefit organizations in performing efficient patch management and prioritize security-related patching as well.

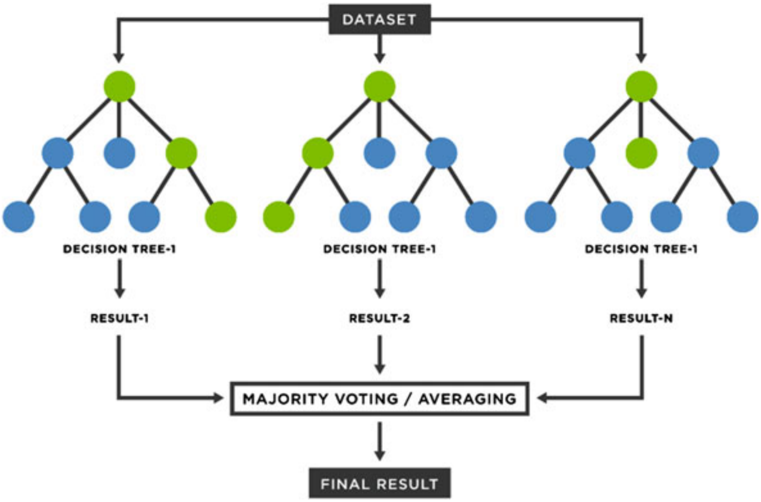

Fig. 9 Random Forest [39]

4.7 Time Lag-Based Modelling for Software Vulnerability Exploitation Process

Only after detection, potential risk can be ill-used. From the moment, the attackers get the information about a new vulnerability that has been discovered, to the final act of exploitation taking place, there exists a finite time lag in between the whole process of exploitation. Using this time lag approach as a benefit, Choudhury et al. [17] developed a model for risk exploitation that takes place in many phases. The time between the detection and exploitation of the vulnerability is limited by the memory kernel function over a finite period of time.

4.8 Session Hijacking Counter Measures

It is said that the attacker takes advantage of the lack of awareness of the user regarding the security of their information or sometimes fools the user to steal their information. The corrective measures for the session hijacking are divided into two layers from the OSI (Open System Interconnection) model:

- Network Layer
- Application Layer

4.8.1 Network Layer

A very crucial step to safeguard our information from getting stolen is always using the Secure Socket Layer that provides end-to-end data encryption. These SSL channels use a 28-bit public key and a 256-bit symmetric key to make encryption tougher and more secure. Even if the attacker gets his hand on the data it will be very difficult to get real data in the pockets.

The use of Secure Socket Shell (SSH) provides a robust authentication and encryption mechanism between two systems on an unprotected network, which helps keep users away from any type of session attack. It is also very important to note that, whenever we visit a website, we must use an HTTPS connection.

4.8.2 Application Layer

According to Sabottke et al. [12] Session ID provides a unique identity for each session and is useful to track user progress and authentication status in the web application. Having a strong and sophisticated Session ID will make it difficult for the attacker to access it. Using a long Session ID by generating one from a random Session ID generator also makes it difficult for the attacker to guess the ID.

4.9 Privacy Set-Up on Social Networking Sites

Long-range social media platforms like Facebook provide many types of privacy settings such as not displaying individual data, for example, mobile number, email ID and so on. These must be updated from time to time from the user's end.

5 Conclusion

In this exploratory analysis, we walked through different possible threats to the security of social media. As more and more users are joining these platforms, it has become a primary cause of lookout for malicious actors. With the increasing amount of data, comes the grave responsibility to keep it secure and this gives a lot of benefits to the attackers while planning to extract valuable and personal information from their target's account. To curb these extensively outspread cybercrimes such as data theft and identity theft, several existing solutions were described in detail. To conclude, social media can become more secure if the users are educated about cybersecurity along with the ongoing efforts made by researchers and analysts to create a secure online environment.

References

1. Das, S., Das, S., Bandyopadhyay, B., Sanyal, S.: Steganography and steganalysis: different approaches (2011)
2. Stokes, K., Carlsson, N.: A peer-to-peer agent community for digital oblivion in online social networks (2013)
3. Mishra, S., Thakkar, H.K., Mallick, P.K., Tiwari, P., Alamri, A.: A sustainable IoHT based computationally intelligent healthcare monitoring system for lung cancer risk detection. Sustain. Cities Soc. **72**, 103079 (2021)
4. Mishra, S., Panda, A., Tripathy, K.H.: Implementation of re-sampling technique to handle skewed data in tumor prediction. J. Adv. Res. Dyn. Control Syst. **10**, 526–530 (2018)
5. Druschel, P., Backes, M., Tirtea, R.: The right to be forgotten—between expectations and practice, Deliverable, ENISA, November 2012 (2012)
6. Weaver, N., Paxon, V., Staniford, S., Cunningham, R.: A taxonomy of computer worms. In: Proceedings of the 2003 ACM Workship on Rapid Malcode (2003)
7. Wang, Y.M., Beck, D., Vo, B., Roussev, R., Verbowski, C.: Detecting stealth software with strider ghostbuster. In: Proceedings of the 2005 International Conference on Dependable Systems and Networks, pp. 368–377 (2005)
8. Forrest, S., Perelson, A.S., Allen, L., Cherukuri, R.: Self-nonself discrimination. In: Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, May 1994 (1994)
9. Tripathy, H.K., Mishra, S., Suman, S., Nayyar, A., Sahoo, K.S.: Smart COVID-shield: an IoT driven reliable and automated prototype model for COVID-19 symptoms tracking. Computing 1–22 (2022)

10. Mishra, S., Mishra, B.K., Tripathy, H.K.: A neuro-genetic model to predict hepatitis disease risk. In: 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1–3. IEEE (2015)
11. Aggarwal, A., et al.: Phishari: automatic realtime phishing detection on Twitter (2013)
12. Sabottke, C., Suciu, O., Dumitras, T.: Vulnerability disclosure in the age of social media: exploiting twitter for predicting real-world exploits. In: Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), pp. 1041–10567 (2015)
13. Sapienza, A., Ernala, S.K., Bessi, A., Lerman, K., Ferrara, E.: DISCOVER: mining online chatter for emerging cyber threats. In: Proceedings of WWW Companion for the Third International Workshop on Computational Methods for CyberSafety, pp. 983–990 (2018)
14. Hartung, F., Kutter, M.: Multimedia watermarking techniques. Proc. IEEE (1999)
15. Tripathy, H.K., Mallick, P.K., Mishra, S.: Application and evaluation of classification model to detect autistic spectrum disorders in children. Int. J. Comput. Appl. Technol. **65**(4), 368–377 (2021)
16. Mishra, S., Dash, A., Ranjan, P., Jena, A.K.: Enhancing heart disorders prediction with attribute optimization. In: Advances in Electronics, Communication and Computing, pp. 139–145. Springer, Singapore (2021)
17. Choudhury, B., Das, R., Baruah, A.: A Novel steganalysis method based on histogram analysis. In: Lecture Notes in Electrical Engineering, pp. 3–4, November 2015
18. Baitha, A.K., Vinod, S.: Session hijacking and prevention technique. Int. J. Eng. Technol. 7(2.6), 193–198
19. Mishra, S., Tripathy, H.K., Thakkar, H.K., Garg, D., Kotecha, K., Pandya, S.: An explainable intelligence driven query prioritization using balanced decision tree approach for multi-level psychological disorders assessment. Front. Pub. Health **9** (2021)
20. Mallick, P.K., Mishra, S., Mohanty, B.P., Satapathy, S.K.: A Deep neural network model for effective diagnosis of melanoma disorder. In: Cognitive Informatics and Soft Computing, pp. 43–51. Springer, Singapore (2021)
21. Alabrah, A., Bassiouni, M.: Preventing session hijacking in collaborative applications with hybrid cache supported one-way hash chains. In: 2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). IEEE (2014)
22. Jain, V., Sahu, D.R., Tomar, D.S.: Session hijacking: threat analysis and countermeasures. In: International Conference on Futuristic Trends in Computational Analysis and Knowledge Management (2015)
23. Sauerwein, C., Sillaber, C., Huber, M.M., Mussmann, A., Breu, R.: The tweet advantage: an empirical analysis of 0-day vulnerability information shared on Twitter. In: Janczewski, L., Kutyłowski, M. (eds.) ICT Systems Security and Privacy Protection, pp. 201–215. Springer (2018)
24. Mondal, S., Tripathy, H.K., Mishra, S., Mallick, P.K.: Perspective analysis of anti-aging products using voting-based ensemble technique. In: Advances in Systems, Control and Automations, pp. 237–246. Springer, Singapore (2021)
25. Mohapatra, S.K., Mishra, S., Tripathy, H.K., Bhoi, A.K., Barsocchi, P.: A pragmatic investigation of energy consumption and utilization models in the urban sector using predictive intelligence approaches. Energies **14**(13), 3900 (2021)
26. Anand, A., Bhatt, N., Kaur, J., Tamura, Y.: Time lag-based modelling for software vulnerability exploitation process (2021)
27. Huber, M., Kowalskiy, S., Nohlbergz, M., Tjoa, S.: Towards automating social engineering using social networking sites, Proceedings of International Conference on Computational Science and Engineering (2009)
28. Kumar, S., Saravanakumar, N., Deepa, K.: On privacy and security in social media—a comprehensive study. In: International Conference on Information Security & Privacy (ICISP2015), 11–12 December 2015, Nagpur, India
29. Tripathy, H.K., Mishra, S., Thakkar, H.K., Rai, D.: Care: a collision-aware mobile robot navigation in grid environment using improved breadth first search. Comput. Electr. Eng. **94**, 107327 (2021)

30. Wang, Z., Huang, D., Zhu, Y., Li, B., Chung, C.-J.: Efficient attribute-based comparable data access control. IEEE Trans. Comput. **64**(12), 3430–3443 (2015)
31. Wu, M.-Y.: On runtime parallel scheduling for processor load balancing. IEEE Trans. Parallel Distrib. Syst. **8**(2), 173–186 (1997)
32. Tian, W., Zhao, Y., Xu, M., Zhong, Y., Sun, X.: A toolkit for modeling and simulation of real-time virtual machine allocation in a cloud data center. IEEE Trans. Autom. Sci. Eng. **12**(1):153–161 (2015)
33. Raja, A.S., Vasanthi, A.: Secured multi-keyword ranked search over encrypted cloud data. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **2**(10) (2012)
34. Mishra, S., Tripathy, H.K., Mallick, P.K., Bhoi, A.K., Barsocchi, P.: EAGA-MLP—an enhanced and adaptive hybrid classification model for diabetes diagnosis. Sensors **20**(14), 4036 (2020)
35. Chattopadhyay, A., Mishra, S., González-Briones, A.: Integration of machine learning and IoT in healthcare domain. In: Hybrid Artificial Intelligence and IoT in Healthcare, pp. 223–244. Springer, Singapore (2021)
36. Ereth, J.: If data is the new oil, metadata is the new gold, 12 April 2017. https://www.eckerson.com/articles/if-data-is-the-new-oil-metadata-is-the-new-gold
37. Black Slash: How to hide secret data inside an image…., 9 July 2018. https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/
38. The Ultimate Guide to Session Hijacking aka Cookie Hijacking, 16 November 2020. https://www.thesslstore.com/blog/the-ultimate-guide-to-session-hijacking-aka-cookie-hijacking/
39. What is a Random Forest? https://www.tibco.com/reference-center/what-is-a-random-forest