

# Systematic review for attack tactics, privacy, and safety models in big data systems

Majdoubi Chaymae, Gahi Youssef, El Mendili Saida

Engineering Sciences Laboratory, National School of Applied Sciences of Kenitra (ENSAK), Ibn Tofail University (UIT), Kenitra, Morocco

## Article Info

### Article history:

Received Jul 8, 2024

Revised Sep 23, 2024

Accepted Sep 30, 2024

### Keywords:

Attacks

Big data

Deep learning

Machine learning

Privacy

Security

## ABSTRACT

This systematic review explores cyberattack tactics, privacy concerns, and safety measures within big data systems, focusing on the critical challenges of maintaining data security in today's complex digital environments. The review begins by categorizing various cyberattacks, laying the groundwork for understanding the threats to big data. It identifies key vulnerabilities that compromise privacy and safety, and examines the ethical implications of these issues. The role of artificial intelligence in enhancing security defenses is highlighted as a crucial aspect of mitigating these threats. Additionally, a comparative assessment of regulatory frameworks such as GDPR, NIST, and ISO 27001 is provided, emphasizing the importance of legal and compliance considerations in data protection. The review concludes by proposing a structured approach to cyberattack detection and processing, advocating for strategies that address both technical vulnerabilities and regulatory requirements, followed by a critical discussion on the usability of previous methods for mobile security, highlighting adaptability and performance, discussing explainability and Gen AI adoption. This work offers valuable insights for researchers, practitioners, and policymakers, contributing to the ongoing discourse on cybersecurity in the big data era.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Majdoubi Chaymae

Engineering Sciences Laboratory, The National School of Applied Sciences of Kenitra

University of Ibn Tofail

B.P: 242 Kenitra, Morocco

Email: chaymae.majdoubi@uit.ac.ma

## 1. INTRODUCTION

As of January 2024, the global internet user count reached 5.35 billion, representing approximately 66.2 percent of the world's population (Digital 2024: Global Overview Report, datareportal). These figures underscore the profound connectivity of our current era, characterized by the pervasive trends of digitalization and globalization. Consequently, the essence of big data era [1]. Many attempts aimed standardizing the definition of big data [2]. As it generally refers to vast and complex datasets surpassing the capacity of data processing systems traditionally used. These datasets are characterized by tremendous volume, velocity, variety, and veracity of data. In the context of data security, big data presents unique challenges and considerations due to its sheer size and the diverse types of information it encompasses. Big data characteristics are developing from three characteristics, five [3], seven [4], and even ten [5].

Table 1 presents characteristics or 10 Vs of big data, as they seem to be the results of researchers out of the three main ones, especially when zoomed in on their definitions; some being sub-characteristics of others becomes noticeable. All this Data advancement raises questions about confidentiality, integrity and authentication (CIA) preservation [6], data privacy, and security; such as unauthorized access, data

interception, data tampering, Denial of Service (DoS) Attacks, and compliance with data protection and privacy regulations.

Table 1. Big data 10Vs

Characteristics	Definition
Volume	Points to the enormous volume of data
Velocity	Represents rapid generation of data and the imperative to promptly process and analyze it in near-real-time or the real one.
Variety	Data types and formats' diversity.
Veracity	The quality and trustworthiness of data.
Value	The need to derive meaningful insights and value from Big Data.
Variability	Describes the inconsistency in data flows.
Visibility	Refers to the challenge of gaining a comprehensive view of data across an organization.
Vulnerability	Acknowledges the privacy and security concerns associated with Big Data.
Validity	Emphasizes the importance of ensuring data is valid and conforms to the rules and constraints of its intended use.
Volatility	Addresses the temporary nature of certain data.

Big data models, integral to data-driven decision-making, face diverse threats seeking to compromise their accuracy and integrity [7]. Adversarial attacks involve manipulating input data to mislead models [8], while data poisoning injects misleading information during the training phase [9]. Model inversion attacks targets deducing sensitive details about training data from outputs of the model [10], and evasion attacks deceive models without altering their underlying structure [11]. Other risks include membership inference attacks, model stealing attempts, backdoor insertion, and Sybil attacks creating fake identities to introduce biased data. Additionally, concept drift attacks exploit changes in data distribution [12], and supply chain attacks target various stages of model development or deployment [13]. Safeguarding against these threats, it is important to be documented about their tactics, be informed on robust security measures, ongoing testing, and collaboration between data scientists and cybersecurity experts to address emerging risks and maintain the resilience of big data models [14].

Despite the progress made, several challenges remain unresolved. The increasing sophistication of attack tactics, such as adversarial, poisoning, and inversion attacks, continues to outpace the development of effective countermeasures. Existing security frameworks often fail to address the full spectrum of threats that target big data environments, particularly when considering the dynamic nature of these systems and the continuous evolution of attack methods. Moreover, the integration of AI into security strategies, while promising, is still in its infancy and requires further research to optimize its effectiveness in detecting and mitigating these threats. Additionally, the regulatory and ethical implications of these emerging threats, particularly in relation to global data protection standards, remain underexplored.

Unlike previous studies that focus on individual attack tactics or isolated privacy measures, this review paper provides a holistic approach by combining AI's capabilities with cybersecurity practices to mitigate advanced threats. The objective is to help understand attacks tactics, expose some privacy and safety measures to overcome these threats, highlighting the use of artificial intelligence to save time and processing efforts, and underscores the importance of adhering to regulations, providing a short comparison or case study to know the use cases of each. Finally end up with providing some technical tools that can be adopted in this context of research for empiric studies.

To emphasize our vision, the rest of the paper is organized following IMRaD style: section 1 introduces the topic, issues, solutions and paper contribution. Section 2 presents review method. Section 3 provides results of main findings, discussions addressing research questions mentioned in section 2 and a critical discussion on previous sections main ideas while projecting on mobile security. To finally conclude in section 4 with main points and future insights.

## 2. REVIEW METHOD

This systematic review follows three main phases: planning, conducting, and reporting [15].

### 2.1. Review planning

In order to address the issue of data privacy and safety based on attacks tactics and used models, our preliminary research questions (RQ) are as follows:

RQ 1: What are the main types of attacks and how can we preserve the privacy and safety of data?

RQ 2: How can we merge artificial intelligence with big data security?

RQ 3: To what extend good practices are important for preserving data security and privacy in Big Data systems?

RQ 4: Are existing frameworks enough to ensure data privacy and safety?

For this purpose, we have conducted the research in different e-resources; Web of Science, Scopus, IEEE Xplore Digital Library, Springer Link, Science Direct, Springer, Wiley Inter Science, Google Scholar, ACM Digital Library, IJEECS, for paper relevance.

Based on research questions and paper keywords, we have used the following strings to localize our review position from the resources: Attacks AND privacy models AND safety models, attacks AND tactics AND safety AND models AND privacy AND models, attacks AND safety AND privacy, attacks tactics, privacy models, security models, attacks tactics, safety, and privacy models, attacks tactics, privacy models, safety models, attacks tactics, safety and privacy models.

Inclusion criteria include paper interest, clear stated objectives, matching the context of studies, date of publication, relevance, quality, citations in some cases. Excluding out dated papers and unmatching paper interests.

## 2.2. Review conduct

Using keywords related to the matter, sorting by relevance and paper purpose alignment. The research methodology has started from general readings to specific readings based on paper date, relevance, matching paper purpose and specific requirements. Our topic previous works research process can be summed up as follows in Figure 1.

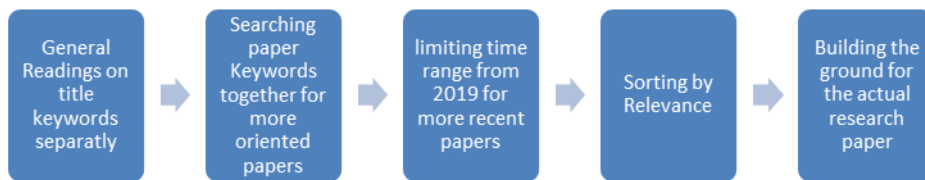


Figure 1. Review conduct process

Across several academic databases, such as Web of Science, Scopus, Science Direct, and Springer, there has been significant scholarly attention dedicated to the realms of attacks, privacy models, and safety models. In Web of Science, for instance, 430 documents encompass these subjects, with 182 being openly accessible. Over the span of 2019 to 2023, there has been a notable increase in the number of documents available. Similarly, in Scopus, a thorough search yielded 955 documents spanning the years 2019 to 2024, particularly prevalent in computer science and English. Science Direct also provides a rich repository of research, with 125 documents concerning attack tactics and a substantial 16,827 documents on open access privacy models from 2019 to 2024. Springer's database, too, highlights the depth of investigation, with 4,011 articles focused on attack tactics and an impressive 49,275 on privacy models from 2019 to 2023. Furthermore, safety models emerge as a significant area of inquiry, with 222,561 results found exclusively on Springer. When considering the collective findings from these databases, it underscores the profound scholarly interest and prolific research output surrounding the nexus of attacks, privacy models, and safety models. Data synthesis in Figure 2 demonstrates open-source references in main used resources, after necessary filters from Table 2.

## OPEN SOURCE DOCUMENTS FROM 2019 TO 2025

■ Web of Science ■ Scopus ■ Springer ■ Science Direct

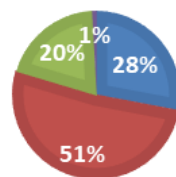


Figure 2. Open-source documents from 2019 to 2025

**2.3. Review reporting**

Table 2 presents a summary of used filter per database. After necessary filters, relevance, paper interest, structured data and approaches, we have used a sum of 80 research paper matching our interests and quality standards, to elaborate this systematic review, making sure to go from general readings to answering our research questions and highlighting the objective mentioned in the introduction section.

Table 2. Review reporting summary

Source	Keywords	Additional filters	Results
Web Of Science	Attacks AND Privacy Models AND Safety Models	keywords	430
		Open Access	182
		From 2019 to 2023	140
		2019	8
		2020	29
		2021	32
		2022	42
Scopus	Attacks AND Tactics AND Safety AND Models AND Privacy AND Models AND Safety AND Privacy	2023	29
		From 2019 to 2024	1
		+ Computer Science	955
Science Direct	Attacks tactics	+ English	806
		From 2019 to 2024 + Computer&Security	794
Springer	Privacy models	Open access + from 2019 to 2024	125
		from 2019 to 2025, open source, Procedia Computer Science	16,827
		Attacks tactics, safety, and privacy models	2,691
Springer	Security models	Attacks tactics, safety, and privacy models	12
		Attacks tactics	12
		From 2019 to 2023, English, sorted by relevance	4,011
		From 2019 to 2023, English, sorted by relevance	49,275
Springer	Safety models	From 2019 to 2023, English, sorted by relevance	222,561
		Attacks tactics, safety and privacy models	302

**3. RESULTS AND DISCUSSION**

This study investigates the effects of the usage of artificial intelligence for preserving privacy and safety, highlighting different types of attack tactics and providing some recommendations, emphasizing on regulatory importance. While earlier studies have explored these matters separately, they have not explicitly addressed these issues in a holistic manner, providing a macro vision for further research. This section explores how the findings of this study can contribute to future research endeavors. It also identifies specific areas where further investigation can be pursued by researchers, addressing research questions.

**3.1. Main types of attacks, privacy and safety measures**

Cyberattacks can employ various tactics and techniques to compromise systems, steal data, or disrupt operations. We cite bellow some common tactics that attackers use:

**3.1.1. Social engineering tactics**

Social engineering attacks manipulate human psychology to obtain sensitive information, using techniques like phishing, pretexting, and advanced persistent threats (APT) [16]. Studies identify key psychological triggers in Vishing attacks, such as authority, distraction, and deception [17]. These attacks follow a lifecycle, from investigation to execution, and often leave little trace (Social Engineering Attacks: The 4 Stage Lifecycle & Common Techniques, Splunk). Awareness campaigns and understanding attacker behavior are common methods to mitigate attacks [18]–[20]. However, these strategies rely on users' ability to recognize threats, which can be inconsistent, especially in high-stress situations.

Automated machine learning (ML) methods like LDA [21], CNN [22], and deep learning classifiers [23] offer scalability and earlier detection, yet depend on high-quality training data and struggle with the interpretability of complex models. Blacklisting known URLs [24] and heuristic classifiers [25] provide quick detection for established threats but lack flexibility against new attack vectors.

Both blacklists and heuristics are reactive, failing to adapt to evolving tactics used by attackers. A hybrid approach integrating user education with ML systems could offer a comprehensive defense. Machine learning models, enhanced with explainable AI (XAI) techniques, would improve interpretability, while adaptive systems using cross-validation [26] and continuous updates [27] would ensure resilience against emerging threats. Combining human-centric awareness with intelligent detection methods is essential for a robust defense against social engineering attacks.

### 3.1.2. Exploiting weaknesses

Exploiting weaknesses in privacy and safety can have severe and far-reaching consequences, impacting both individuals and organizations, as it is one of the widely used tactics, such as exploiting vulnerabilities; when attackers look for weaknesses in software, operating systems, or network configurations to gain unauthorized access [28], privilege escalation, exploiting zero-day vulnerabilities [29] or known security flaws, Insider threats, hazardous threats [30], targeting websites or online platforms that are frequented by the target audience to infect visitors, or using watering holes attacks withing its five stages, Splunk: Gathering intelligence, Analyzing the intel, Preparing the attack (attacks are often SQL injection, XSS, zero-day exploitation), executing the attack (malware APT); Targeting vulnerabilities in internet-connected devices to gain control or disrupt their functioning.

For this matter it is important to improve vulnerability detection, via prediction [31], using vulnerability scoring system such as CVSS [32], [33], machine learning based frameworks [34], or sensitive systems' isolation [35]. AKO (the additional kernel observer) [36] was one of the solutions used for privilege escalation prevention or detection ways [37] as [38] in cloud, exposing insider threat classification algorithms. Various methods to evade detection by security software or monitoring systems were deployed, such as polymorphic malware or rootkit installation [39]. Insider threats earlier detection [40] is one of the most recommended prevention techniques [41]. Using detection measures is important, static or dynamic methods for android as an example, nevertheless their actual limitations in terms of unpredicted evasions [42].

### 3.1.3. Authentication attack

Authentication attacks can have significant privacy and security impacts, as they target the processes and mechanisms used to check users' identity of and entities accessing a system. For example, password attacks are about attempting to crack or guess passwords to gain access to accounts or systems [43]. Common techniques include brute force attacks [44], dictionary attacks [45], and credential stuffing or stealing login credentials through various means, such as keyloggers, phishing, or password spraying [46] were used for this purpose. Therefore, to avoid password attacks, it is recommended to use some solutions, such as SGX-unified access management (UAM) [47], access management in IOT via the implementation of PinWheel [48] ensuring privacy and security, password based credential (PBC) [49], or reflexive memory authenticator [50].

### 3.1.4. Malicious software deployment

Malicious software deployment, commonly referred to as malware, can have profound effects on privacy and safety, for a malware is designed with malicious intent, as its impact can vary from stealing sensitive information to causing significant disruptions; viruses, worms, trojans, or ransomware compromise the target system. On the one hand, a malware can be delivered through email attachments, infected websites, or compromised downloads [51], [52]. Therefore, adversarial attacks and defenses are used for malware detection [53], in addition to edge computing and DL malware detection for IoT [54], and forensic neural networks for malware localization [55]. On the other hand, drive-by downloads are Infecting a user's computer or device when they visit a compromised or malicious website, often without their knowledge or consent [56]. Twitter has faced this event before [57], [58], therefore detection measures were a good research path to optimize it [59]. However, many solutions were used to address rogue wireless access points, such as the blockchain-encryption-based solutions to protect fog federations [60].

### 3.1.5. Network manipulation

Network manipulation can have significant effects on both privacy and safety, as it involves the intentional alteration or interference with network communication. For example, overloading a target system or network with excessive requests to render it unavailable to legitimate users, DDOS attacks on cloud or software defined networks (SDNS) [61], Intercepting and eavesdropping on communications between two parties, often without their knowledge, to steal or manipulate data, session hijacking. To limit its effect, it is important to deploy detection mechanisms, considering counter measures and investing in DOS mitigation services [62]–[64]. Using multipath transmission control protocol (MPTCP) [65], or detection measures such as Echo analysis [66], artificial neural networks [67]–[69].

### 3.1.6. Web application exploitation

Web application exploitation can have severe consequences for both privacy and security, by taking advantage of vulnerabilities in web applications to gain unauthorized access, manipulate data, or compromise the overall integrity of the system. For example, exploiting poorly sanitized inputs in web applications, gaining unauthorized access to databases and manipulate data [70], injecting malicious scripts into web pages, which are then executed by other users' browsers, potentially leading to data theft or manipulation.

In order to detect and optimize SQL injection effect, in a smart connected environment, the use of artificial intelligence is compromising, such as automating penetration testing using GANS [71] or deploying artificial neural networks for SQL injection detection, such as the solution suggested in [72], using convolutional neural networks. Semantic parsing is used for server-site [73], using machine learning techniques such as hybrid learning for XSS detection [74], as well as Knuth-Morris-Pratt string match algorithm [75] for SQL injection and cross-site scripting detection.

### 3.1.7. Digital media exploitation

Exploiting digital media presents substantial challenges to safety and privacy, encompassing a range of risks. This involves unauthorized entry into personal information, resulting in privacy violations and potential issues like identity theft, cryptojacking. The improper use of digital media can contribute to online harassment and cyberbullying, causing emotional harm and harm to one's reputation. Data breaches, stemming from unauthorized access and exploitation of digital content, expose individuals to financial and identity risks. Additionally, the creation of deceptive or harmful content, taking advantage of security vulnerabilities, and phishing attacks further jeopardize safety and privacy. Violating privacy laws may result in legal repercussions, including fines. Furthermore, the psychological impact on individuals, such as stress and anxiety, emphasizes the broader implications of digital media exploitation on mental health. Addressing these challenges requires a comprehensive approach, including legal measures, enhanced cybersecurity, and increased user awareness to promote responsible and ethical use of digital media. Social Media Manipulation is creating and spreading disinformation or propaganda on social media platforms to influence public opinion or conduct targeted attacks [76]. It is important to take some prediction actions as well as counter measure considerations, for truth manipulation [77] or decision making [78]. In the coming section, results will be classified depending on attacks occurrence, good ethics and suggested Artificial Intelligence tools to address it.

## 3.2. Artificial intelligence use for big data security and good practices for data security and privacy

In the previous subsection, we have discussed types of attacks and used means to preserve data privacy and safety, the use of Artificial Intelligence was underscored in different occasions. In Table 3, we will provide a comparative chart of different attack types, occurrence and use of AI as well as recommended good practices.

The occurrence is compared to "all sectors" and based on ENISA 2023 report. For DDOS Attacks percentage, we have calculated the average of provided sectors to make it an 'all sectors' result, considering an equal importance to provided sectors. 96% of phishing attacks arrive by email, TESSIA. According to SYMANTEC research, in 2020; 1 in every 4,200 emails is a phishing one. Modern attacks often occur using artificial intelligence; therefore, we see that enhancing intelligent, automated solutions would be a beneficial way to protect our data and generate instant responses. Attackers often combine multiple tactics and techniques to achieve their goals. Defending against cyberattacks requires a multi-faceted approach, including robust cybersecurity measures, regular security updates, and user education and awareness. For watering holes artificial intelligence solution, we suggest using adversarial attacks responses, GANS for automation [79]. Based on the definition we have provided above, Combination of malware solutions, SQL injection, XSS, Zero-day exploitation can be beneficial for such composite attacks.

For Phishing occurrence and spear phishing, the statistic is taken from Sophos investigation, involving 3,000 Chief Information Officers and Chief Security Information Officers across 14 countries. All participants (United States, Japan, United Kingdom, Germany, India, Austria, South Africa, France, Spain, Australia, Brazil, Singapore, Italy, Switzerland) were affiliated with organizations ranging from 100 to 5,000 employees. The survey, conducted by the Vanson Bourne agency, took place during January and February of 2023. Main findings were as follows:

The predominant risk lies in data exfiltration, accounting for 41%, followed closely by phishing, including spear phishing, at 40%. Ransomware poses a significant threat at 35%, while cyber extortion and DDoS attacks contribute in risks at 33% and 32%, respectively. The compromise of business email (BEC) is identified as a concern at 31%. Active adversaries, those manually orchestrating attacks, constitute a threat at 30%, along with mobile malware at the same percentage. Cryptominers and wipers pose risks at 22% and 16%, respectively. The category labeled "others" accounts for 0%, and notably, a minimal 1% express no fear of cyber threats affecting their companies in 2023, while 0% remain uncertain about the potential impact.

After getting to know more about attacks tactics, good ethics, the use of artificial intelligence for data privacy and safety, a projection on Big Data environment is mandatory to understand these threats in depth and concerned big data models per threat classification as presented in Table 4.

Table 3. Attacks, occurrence, good ethics and AI usage

Attacks	Good Ethiques	Artificial intelligence	Occurrence	Comment/Additional
Phishing	Anti-phishing Environment	Cross-validation classification	40%	Prediction and Detection using ML
Social Engineering	Spreading Awareness, understanding Attacker's behavior	Latent Dirichlet Allocation (LDA), CNN, DL and ML classifiers Methods	8%	Early detection, blacklisting using manually verified URLs
Exploiting Vulnerabilities	Vulnerability Scoring System (CVSS)	ML based Framworks, Prediction, Vulnerability Prediction Model [79]	+50% of high risk exploited vulnerabilities, (2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is)	Sensitive system isolation
Password Attacks	Access Management		2021 – Identification and Authentication Failures: Max Coverage: 79.51%	Analysis of 1.8 million passwords reveals 40,000 occurrences of 'admin' as default password, CentralBay. Use of AI for Detection
Malware Deployment		Adversarial Attacks and defenses, DL detection metods, Forensic Neural Networks for malware localization	11% Mobile malware: 30%, Sophos	
DOS and DDOS	Investing in solutions	Dos mitigation, detection	20% ENISA 32% Sophos	First occurrence is based on ENISA results, the second is explicitly mentioned on Sophos study.
Man-in-the-Middle (MitM)	Echo analyses	Multipath Transmission Control Protocol	5 billion records, Cognyte. 5 billion records, Twitch. 700 million records, LinkedIn. 553 million records, Facebook	<ul style="list-style-type: none"> <li>The use of ANN is recommended</li> <li>MIT has contributed to the largest breaches in 2021, Fortinet</li> </ul>
SQL injection	Process automation	ANN, CNN detection, GANS	42%, EdgeScan	Automating Penetration testing using GANS
XSS		Hybrid learning detection, Knuth-Morris-Pratt string match algorithm	9%, Cloudflare	
Social Media Manipulation	Awareness	Prediction, decision making, truth detection		
Privilege Escalation	Good management	Additional kernel observer, insider threat classification Algorithms	80% of security breaches involve privilege escalation, Vectra AI	Detection in cloud using ML (LightGBM Insider threat Classification), solutions highest accuracy 97%
Evasion Techniques	Using human experience	Maaker Framework		Android evasions detection techniques have limitations
Watering Hole	Users should reevaluate their third-party services, network access management	Combination of malware solutions, SQL injection, XSS, Zero-day exploitation.	23%	Uses open windows instead of doors
IoT Device Exploitation		HALE-IoT, detection and prevention techniques	Every week, organizations witness 54% average of attempted attacks on IOT devices.	
Credential Theft	Password Based credential			Reflexive Memory Authenticator
Rogue Wireless Access Points		Blockchain-Encryption-Based Approach		
Drive-By Downloads		Detection		
Insider Threats	Prevention	Earlier Detection	74% of organizations' vulnerabilities, The 2023 Insider Threat report	

Security threats present substantial risks to the reliability, performance, and integrity of big data models. Various forms of attacks, such as data poisoning, adversarial attacks, and denial-of-service incidents,

can compromise the accuracy of these models. Data poisoning involves injecting harmful data into the training set, impacting the model's predictive abilities. Adversarial attacks manipulate input data to deceive the model, undermining its resilience and adaptability. Denial-of-service attacks target the infrastructure, causing service disruptions and potential financial losses. These attacks not only jeopardize prediction accuracy but also raise concerns about privacy [80], intellectual property theft, and the overall dependability of big data models. Effectively mitigating these risks necessitates the implementation of robust security measures, ongoing monitoring, and the integration of privacy-preserving techniques [81] to ensure the resilience of big data models in the face of evolving cybersecurity threats.

Table 4. Attacks classification per concerned big data models

Attack type	Famous attacks	Big data concerned models
Social Engineering Tactics	<ul style="list-style-type: none"> <li>- Social Engineering</li> <li>- Phishing</li> <li>- Pretexting</li> <li>- Baiting</li> <li>- Tailgating</li> </ul>	<ul style="list-style-type: none"> <li>- Machine Learning Models</li> <li>- Deep Learning Models</li> <li>- Predictive Analytics Models</li> <li>- Natural Language Processing (NLP) Models</li> <li>- Graph Analytics Models</li> <li>- Cluster Analysis Models</li> <li>- Anomaly Detection Models</li> <li>- Recommender Systems</li> <li>- Time Series Analysis Models</li> <li>- Collaborative Filtering Models</li> </ul>
Exploiting System Weaknesses	<ul style="list-style-type: none"> <li>- Exploiting Vulnerabilities</li> <li>- Insider Threats</li> <li>- Privilege Escalation</li> <li>- Evasion Techniques</li> <li>- Watering Hole Attacks</li> <li>- IoT Device Exploitation</li> </ul>	<ul style="list-style-type: none"> <li>- Machine Learning Models</li> <li>- Deep Learning Models</li> <li>- Predictive Analytics Models</li> <li>- Natural Language Processing (NLP) Models</li> <li>- Graph Analytics Models</li> <li>- Cluster Analysis Models</li> </ul>
Authentication Attacks	<ul style="list-style-type: none"> <li>- Password Attacks</li> <li>- Credential Theft</li> </ul>	<ul style="list-style-type: none"> <li>- Anomaly Detection Models</li> </ul>
Malicious Software Deployment	<ul style="list-style-type: none"> <li>- Malware Deployment</li> <li>- Drive-By Downloads</li> <li>- Rogue Wireless Access Points</li> </ul>	<ul style="list-style-type: none"> <li>- Recommender Systems</li> <li>- Time Series Analysis Models</li> <li>- Collaborative Filtering Models</li> <li>- Ensemble Models</li> </ul>
Network Manipulation	<ul style="list-style-type: none"> <li>- DoS, DDoS</li> <li>- MitM</li> <li>- Session Hijacking</li> </ul>	
Web Application Exploitation	<ul style="list-style-type: none"> <li>- SQL Injection</li> <li>- Cross-Site Scripting (XSS)</li> </ul>	
Digital Media Exploitation	<ul style="list-style-type: none"> <li>- Social Media Manipulation</li> <li>- Cryptojacking</li> </ul>	<ul style="list-style-type: none"> <li>- Image Recognition Models</li> <li>- Video Analysis Models</li> <li>- Audio Processing Models</li> <li>- Deepfake Generation Models</li> <li>- Social Media Analysis Models</li> <li>- Content Recommendation Models</li> <li>- Augmented Reality (AR) Models</li> <li>- Interactive Multimedia Models</li> <li>- Biometric Recognition Models</li> <li>- Media-based Behavioral Analytics Models</li> </ul>

**3.3. Existing frameworks comparison**

Many frameworks were taken into consideration either by scientists, researchers, and field contributors to provide better safety and privacy measures. However, it is important to understand main market competitors for data protection regulations to know better use cases per each. Table 5 thoroughly compares three essential frameworks focused on data protection and cybersecurity: the general data protection regulation (GDPR), the National Institute of Standards and Technology (NIST) cybersecurity framework, and the International Organization for Standardization (ISO) 27001. The goal is providing a nuanced understanding of these frameworks, considering their focus, applicability, enforcement mechanisms, and additional dimensions.

This markdown chart provides a clear and organized presentation of the comparative analysis of the GDPR, NIST cybersecurity framework, and ISO 27001. Adjustments can be made as needed for your specific context. Enhancing data protection based on these regulations, compliance, big data context is more realistic, as we deal with the fusion of different aspects that can't be independent one from the others. The



coming subsection provides a generic approach for cyberattacks detection and processing, limitations and good practices.

Table 5. Comparative Analysis of some data security and privacy frameworks

Aspect	GDPR	NIST cybersecurity framework	ISO 27001
Emphasis/Focus	Safeguarding personal data and privacy rights	Comprehensive approach to managing cybersecurity risks	Addressing Information Security Management Systems (ISMS)
Key Principles/Components	Consent, data minimization, purpose limitation, accuracy, storage limitation, integrity, confidentiality   Functions: Identify, Protect, Detect, Respond, Recover	Functions: Identify, Protect, Detect, Respond, Recover	Risk assessment, security policy, organizational structure, asset management, access control, cryptography, incident response, continuous improvement
Enforcement Mechanisms	Stringent enforcement, fines for non-compliance	Voluntary nature, no legal mandate for adherence	Option for certification, signaling alignment with standard
Applicability Scope	European Union primarily, global impact	International, not tied to a specific region	International
Legal Jurisdiction	European Union	United States (U.S.)	International
Voluntariness	Mandatory	Voluntary	Voluntary
Flexibility and Adaptability	Specific requirements for compliance	Adaptable to various organizational structures and industries	Flexible and adaptable to organizational needs
Integration with Other Standards	-	Ease of integration not explicitly defined	Integration with other standards is possible
Frequency of Updates	-	Not specified	Continuous improvement; updates as needed
Implementation Challenges	-	Challenges may vary; not explicitly defined	Challenges may vary; not explicitly defined
Cost of Implementation	-	Costs not explicitly defined	Costs not explicitly defined
Public Perception and Trust	Compliance seen positively, builds trust	Positive perception; adherence viewed as best practice	Positive perception; certification enhances credibility
Audit and Certification Process	Rigorous audit process: certification required	No specific certification, self-assessment encouraged	Certification is optional, organizations may seek it

### 3.4. Structured approach to cyberattacks detection and processing

To detect cyberattacks and try to process it, it is important to combine different aspects mentioned before like considering data variability, attacks properties, big data context, regulation means. To have a global image of context variables before trying to solve the issue. Therefore, we suggest the following process presented in Figure 3.

In the first stage; Holistic Data Collection and Enrichment, the focus is on aggregating data from various sources and then enriching and normalizing the data for consistency across the entire system. Key data sources include network traffic logs (e.g., NetFlow data, pcap files), system logs (e.g., server syslogs, firewall logs), threat intelligence feeds (e.g., STIX, TAXII), and user behavior analytics (e.g., endpoint device logs, access patterns). Tools such as Kafka or Flume can handle real-time data ingestion, while Hadoop or Spark can store and process large datasets. Data flow management and enrichment are facilitated by NiFi. During this stage, the primary metrics to monitor include the volume of data collected, the time required for data normalization, and the consistency and completeness of enriched data. Figure 4 presents examples of tools to be used in this context.

The second stage; advanced analytics and machine learning, involves applying advanced machine learning techniques for real-time anomaly detection and attack recognition. Tools like Scikit-learn, TensorFlow, and PyTorch are leveraged to train machine learning models, while the ELK Stack (Elasticsearch, Logstash, Kibana) helps with data analytics and visualization. For scalable machine learning, frameworks like Spark MLlib or H2O.ai come into play. The experimental process entails training models using labeled datasets such as NSL-KDD and CICIDS2017 to identify known attack patterns. Once trained, these models are tested on real-time streaming data for anomaly detection. Metrics to monitor here include detection accuracy, false-positive and false-negative rates, and model training time. Figure 5 demonstrates examples of ML libraries for anomaly detection, classification and ML models for scalability and portability.

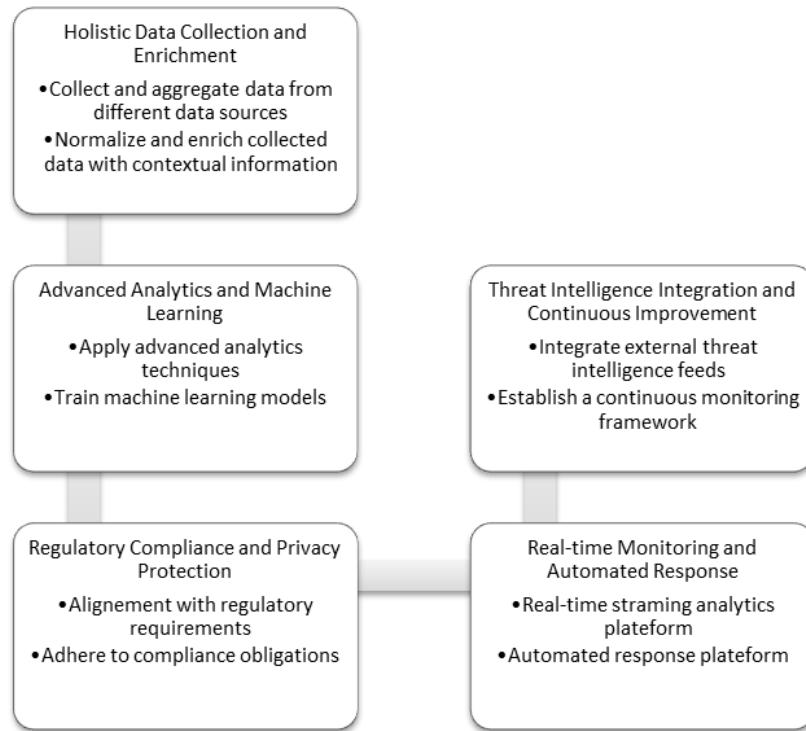


Figure 3. A structured approach to cyber-attacks detection and processing



Figure 4. Data collection and enrichment process



Figure 5. ML libraries for anomaly detection, classification and ML models for scalability and portability

Ensuring compliance with data protection regulations like GDPR and ISO 27001 is a critical part of the setup. Tools like Apache Ranger or Apache Sentry can enforce role-based access control (RBAC) and data governance, while data masking and encryption tools (e.g., VeraCrypt, GnuPG) are used for anonymization and pseudonymization of sensitive data. This stage’s metrics focus on compliance with GDPR standards, specifically data anonymization and access control, and the overall effectiveness of data protection measures. Figure 6 provides encryption examples and access control mechanisms.

At the stage of real-time monitoring and automated response, the system implements real-time monitoring of incoming data streams and automates responses to detected incidents. Tools like Apache Storm or Apache Flink enable real-time stream processing, while SOAR platforms (Security Orchestration, Automation, and Response) such as Phantom or Demisto automate incident response. Additionally, intrusion detection systems like Snort or Suricata help detect network-level threats. Key metrics to monitor here are the time taken to detect anomalies, response time to incidents, and the effectiveness of automated responses (e.g., quarantining devices, blocking IPs). Figure 7 provides examples of real-time monitoring and automated response tools.



Figure 6. Encryption examples and access control mechanisms



Figure 7. Examples of real-time monitoring and automated response tools

The final stage; Threat Intelligence Integration and Continuous Improvement, integrates external threat intelligence feeds to enhance detection capabilities. Tools like malware information sharing platform (MISP) allow for threat intelligence sharing, and STIX/TAXII standards are employed to ingest external threat data. The experimental process involves incorporating external threat data into the detection pipeline and continuously refining detection models based on feedback from live incidents. Metrics in this stage include improvements in detection rates following threat feed integration and the time taken to incorporate new threat intelligence data. Figure 8 presents threat intelligence integration and continuous improvement.

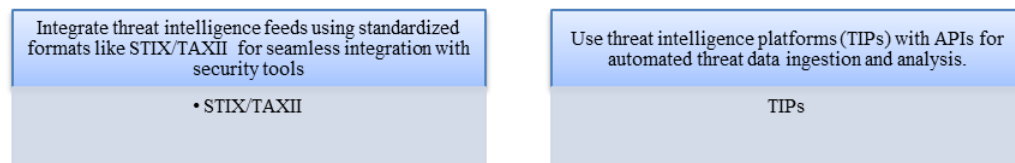


Figure 8. Threat intelligence integration and continuous improvement

Through the fusion of big data analytics with principles from NIST, GDPR, and ISO 27001, organizations can establish a refined process for detecting and managing cyber threats, mitigating risks, safeguarding sensitive data, and ensuring adherence to regulatory standards, all while harnessing the scalability and adaptability of big data systems to combat the dynamic threat landscape.

The experimental environment requires high-performance servers for data storage, processing, and machine learning model training. Networking equipment such as switches and routers simulate real-world network traffic and attacks. Datasets like NSL-KDD and CICIDS2017 are used for training and validation. Additionally, the setup simulates various types of cyber-attacks (e.g., DDoS, SQL injection, privilege escalation, insider threats) to assess the detection and response system's effectiveness. Throughout the experiment, key performance indicators (KPIs) are tracked to evaluate system performance. These include detection accuracy (the percentage of correctly identified attacks), response time (the time between attack detection and automated response), regulatory compliance (adherence to privacy and data protection laws), and scalability (the system's ability to handle large volumes of data without a performance drop).

### 3.5. Critical discussion and mobile security extension

The critical discussion of the current paper is structured as the following framework: types of attacks and tactics for general and mobile security, privacy and safety, good practices, explainability and Gen AI for data security and privacy.

#### 3.5.1. Types of attacks

The paper discusses main types of attacks, the preliminary plan concerned of more attacks tactics than provided, but the priority was to more documented attacks to have more data reliability. The mentioned attack tactics are highly relevant to mobile security. Social engineering attacks, such as phishing through

SMS or social media, trick users into revealing sensitive information or installing malicious apps. Mobile devices with unpatched vulnerabilities are exploited by attackers to gain unauthorized access. Authentication methods, including passwords and biometric data, are targeted by attacks like credential stuffing or SIM swapping. Malicious software, often disguised as legitimate apps, is used to steal data or control devices. Network-based attacks, such as man-in-the-middle (MITM) attacks, exploit unsecured Wi-Fi connections. Mobile web applications and browsers are vulnerable to exploitation through techniques like cross-site scripting (XSS) or SQL injection. Additionally, attackers use infected digital media to exploit vulnerabilities in media handling software, compromising mobile devices.

Table 6. Main mobile attacks

Attack classification	Attack type
Application-based attacks	<ul style="list-style-type: none"> <li>- Malware: Malicious software disguised as legitimate apps can steal data, spy on users, or take control of the device.</li> <li>- Spyware: Apps that secretly collect user data and transmit it to an attacker.</li> <li>- Ransomware: Malicious apps that encrypt user data and demand a ransom to unlock it.</li> <li>- Phishing Apps: Apps that mimic legitimate services to trick users into revealing sensitive information like passwords.</li> </ul>
Network-based attacks	<ul style="list-style-type: none"> <li>- Man-in-the-Middle (MitM) Attacks: Attackers intercept communication between the mobile device and a network to eavesdrop or alter the data.</li> <li>- Wi-Fi Eavesdropping: Attackers create rogue Wi-Fi networks or compromise legitimate ones to intercept data transmitted by the device.</li> <li>- Session Hijacking: Attackers take control of a user session by stealing session tokens during a network transaction.</li> </ul>
Web-based attacks	<ul style="list-style-type: none"> <li>- Drive-by Downloads: Malicious code is automatically downloaded and executed when a user visits a compromised website.</li> <li>- Cross-Site Scripting (XSS): Malicious scripts are injected into web pages viewed on a mobile device, which can then be used to steal cookies or redirect to malicious sites.</li> <li>- Phishing: Fake websites are designed to look legitimate, tricking users into entering sensitive information.</li> </ul>
Device-based attacks	<ul style="list-style-type: none"> <li>- Jailbreaking/Rooting Exploits: Techniques that exploit vulnerabilities to gain root access, allowing attackers to bypass security restrictions.</li> <li>- SIM Swapping: Attackers trick or bribe telecom operators into swapping the SIM card associated with a phone number, allowing them to take control of the victim's accounts.</li> <li>- Bluetooth Attacks: Exploits that use Bluetooth to gain unauthorized access to the device (e.g., Bluejacking, Bluesnarfing, Bluebugging).</li> </ul>
SMS-based attacks	<ul style="list-style-type: none"> <li>- Smishing: Phishing via SMS, where attackers send fraudulent messages to trick users into clicking on malicious links or revealing sensitive information.</li> <li>- Premium Rate SMS: Apps or attackers send SMS messages to premium-rate numbers without the user's knowledge, resulting in excessive charges.</li> </ul>
Social engineering attacks	<ul style="list-style-type: none"> <li>- Fake Security Alerts: Attackers send alerts or warnings, pretending to be legitimate entities, to convince users to install malicious apps or share personal information.</li> <li>- Vishing: Voice phishing, where attackers call users pretending to be from a trusted organization to extract sensitive information.</li> </ul>
Physical attacks	<ul style="list-style-type: none"> <li>- SIM Card Theft: Physically stealing a SIM card to access the victim's accounts and personal information.</li> <li>- USB Attacks: Using USB connections to exploit vulnerabilities in the device, such as installing malware or extracting data.</li> </ul>
Cloud-based attacks	<ul style="list-style-type: none"> <li>- Data Synchronization Exploits: Attacks targeting cloud services where mobile data is stored or synced, leading to data breaches.</li> <li>- Account Takeover: Gaining unauthorized access to cloud accounts associated with the mobile device, leading to data theft or loss.</li> </ul>
Firmware/operating system exploits	<ul style="list-style-type: none"> <li>- Zero-Day Exploits: Exploiting unknown vulnerabilities in the mobile OS or firmware before patches are available.</li> <li>- Bootloader Attacks: Compromising the device's bootloader to install custom firmware that can bypass security protections.</li> </ul>

Table 6 presents mobile attacks categorized based on their targets, vectors, and the used techniques. The comprehensive overview of mobile attack vectors highlights various threats ranging from application-based to firmware-level exploits. Application-based attacks like malware, spyware, and phishing apps target users directly through malicious or deceptive apps. Network-based threats such as Man-in-the-Middle attacks and Wi-Fi eavesdropping exploit communication channels, while web-based threats like drive-by downloads and XSS exploit vulnerabilities in web content. Device-based attacks, including jailbreaking and SIM swapping, compromise device security, while SMS-based and social engineering attacks deceive users into disclosing sensitive information. Physical attacks and cloud-based threats exploit hardware and cloud services, respectively. Firmware exploits, such as zero-day vulnerabilities and bootloader attacks, emphasize the need for timely updates and secure boot processes. Addressing these diverse threats requires a multi-

layered security approach involving secure app development, robust network protection, user education, and continuous vigilance across all layers of mobile technology.

### 3.5.2. Privacy and safety

Privacy and safety frameworks, especially when applied to mobile environments, involve several technical mechanisms and standards designed to protect user data and ensure secure operations. For example, the GDPR mandates technical controls like data encryption and pseudonymization to protect personal data both at rest and in transit. Mobile applications must implement strong cryptographic methods, such as AES (Advanced Encryption Standard) for data storage and TLS (Transport Layer Security) for secure communication channels. Additionally, GDPR's requirement for data minimization encourages developers to adopt techniques like differential privacy, which allows data analysis without exposing individual user data. This is particularly relevant in mobile applications that collect large amounts of user-generated data, such as location or health information.

Mobile-specific frameworks dive deeper into the technicalities of securing applications and devices. The OWASP Mobile Security Framework (MASVS & MSTG), for instance, provides a comprehensive guide for developers to build secure mobile apps. It includes best practices for secure coding, such as input validation and secure session management, to prevent common vulnerabilities like SQL injection or session hijacking. It also emphasizes the importance of implementing secure storage mechanisms, recommending the use of platform-specific secure storage solutions, such as iOS Keychain or Android Keystore, which use hardware-backed encryption to store sensitive data like authentication tokens or passwords. Moreover, OWASP suggests performing regular security testing, including static and dynamic analysis, to identify and mitigate vulnerabilities early in the development lifecycle. These practices ensure that mobile applications not only comply with privacy regulations but also maintain a high level of security, protecting users from various attack vectors like malware, phishing, and unauthorized access.

### 3.5.3. Good practices

Ensuring privacy and safety in any system, whether digital or physical, requires adherence to a set of fundamental best practices that form the backbone of a secure environment. At the core of these practices is data minimization, which involves collecting only the necessary data required for a specific purpose, thereby reducing the risk of exposing unnecessary or excessive information. This principle is closely tied to user consent and transparency, where organizations must clearly communicate their data collection practices to users and obtain explicit consent before any data is gathered. Encryption plays a crucial role in protecting data both at rest and in transit, utilizing strong cryptographic algorithms like AES-256 for storage and TLS 1.2 or higher for secure communications. In addition to these, access control mechanisms such as role-based access control (RBAC) and multi-factor authentication (MFA) ensure that only authorized personnel have access to sensitive data, thereby minimizing the risk of internal breaches. Regular security audits and vulnerability assessments are also essential, as they help identify and mitigate potential risks before they can be exploited by malicious actors. Finally, privacy by design mandates that privacy considerations be integrated into the development lifecycle of any system, ensuring that privacy is not an afterthought but a fundamental aspect of the design process.

When it comes to mobile environments, these general best practices must be adapted and expanded to address the unique challenges posed by mobile devices and applications. Secure app development is paramount, requiring developers to follow frameworks like OWASP MASVS, which provide guidelines on secure coding, including input validation, session management, and secure storage practices. Given the mobile context, permission management is also critical, as mobile apps often request access to various device features, such as location, camera, and contacts. Developers must ensure that apps request only the permissions necessary for their functionality, reducing the risk of misuse. Additionally, data encryption on mobile devices is essential to protect sensitive information in case the device is lost or stolen. This can be achieved using platform-specific tools like iOS Keychain or Android Keystore, which provide hardware-backed encryption. Mobile applications must also secure their communication channels using TLS/SSL to protect data as it travels between the app and backend servers. To further enhance security, mobile operating systems inherently offer sandboxing and application isolation, preventing apps from accessing each other's data. Regular app updates and patching ensure that known vulnerabilities are promptly addressed, while user authentication and biometric security provide strong authentication mechanisms, including multi-factor authentication and biometric options like fingerprint or facial recognition. By integrating these mobile-specific practices, organizations can create a robust defense against the myriad threats that target mobile devices and ensure that user privacy and safety are maintained at all times.

### 3.5.4. Explainability and gen AI

Explainability in AI is crucial for enhancing trust and transparency across various applications, including security. In general security, explainable AI helps users and analysts understand why certain actions or alerts are triggered, improving the accuracy of threat assessments and reducing false positives. This transparency is vital for regulatory compliance, as it allows organizations to demonstrate that their AI-driven decisions are made responsibly based on clear, understandable criteria. In mobile security, explainability ensures users can trust and effectively interact with AI-powered features. AI applications in mobile security, such as those detecting malware and phishing attempts, benefit from explainability by providing users with clear reasons for alerts. This might involve identifying unusual app behavior or matching known malware signatures, helping users make informed decisions about app permissions and security measures.

Looking ahead, general artificial intelligence (Gen AI), or artificial general intelligence (AGI), aims to emulate human-like cognitive abilities, performing any intellectual task a human can. Unlike today's specialized AI, Gen AI would have the flexibility to understand, learn, and apply knowledge across various domains. In security, Gen AI could revolutionize threat detection and response by analyzing complex data patterns from diverse sources, potentially identifying and neutralizing sophisticated cyber threats before they occur. However, developing and deploying Gen AI presents significant challenges. Ensuring these systems are ethical, transparent, and trustworthy is essential. With its advanced decision-making capabilities, understanding how Gen AI reaches its conclusions is crucial for maintaining trust and accountability. Ongoing research will be needed to address these ethical considerations and technical hurdles as the field of Gen AI progresses.

## 4. CONCLUSION AND FUTURE INSIGHTS

This systematic review has explored the critical intersection of cyberattacks, privacy concerns, and safety models within big data systems. Given the rapid expansion of digital technologies and the vast amounts of sensitive data generated, understanding and addressing these issues is crucial for both organizations and individuals. The importance of this topic lies in its direct impact on the integrity, confidentiality, and overall security of big data environments, which are foundational to modern digital infrastructure. Our study underscores the necessity of a layered, adaptive cybersecurity strategy, incorporating advanced analytical techniques, regulatory compliance, and AI-driven defenses. This approach is not only essential for protecting data but also for ensuring that organizations can operate securely in an increasingly interconnected world. The thesis of this review emphasizes that a comprehensive cybersecurity strategy must evolve continually to address emerging threats while balancing the needs for privacy and usability. While some may argue that current security frameworks and practices are sufficient, our analysis reveals significant gaps, particularly in handling the evolving nature of cyber threats and the scalability of big data systems. These gaps highlight the need for continued research and innovation in this field. The study advocates for proactive measures, such as regular updates to security protocols, the integration of AI for real-time threat detection, and adherence to international standards like GDPR and ISO 27001. These steps are essential for mitigating risks and ensuring robust data protection. In conclusion, this review not only provides insights into the existing challenges but also calls for ongoing research to address the limitations identified. Future research should focus on improving the scalability of security measures, developing more sophisticated threat detection models, and exploring the ethical implications of big data security. By prioritizing these areas, researchers and practitioners can help build a more secure and privacy-conscious digital landscape. Main questions for coming works are related to the adaptability of different platforms to security measures especially at the performance level of different mobile attacks, mitigating risks and contributing to boosting security and privacy levels.

## REFERENCES

- [1] Z. A. Al-Sai *et al.*, "Explore big data analytics applications and opportunities: a review," *Big Data and Cognitive Computing*, vol. 6, no. 4, 2022, doi: 10.3390/bdcc6040157.
- [2] M. Al-Mekhlal and A. Ali Khwaja, "A synthesis of big data definition and characteristics," in *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Aug. 2019, pp. 314–322. doi: 10.1109/CSE/EUC.2019.00067.
- [3] M. Younas, "Research challenges of big data," *Service Oriented Computing and Applications*, vol. 13, no. 2, pp. 105–107, Jun. 2019, doi: 10.1007/s11761-019-00265-x.
- [4] I. El Alaoui and Y. Gahi, "The impact of big data quality on sentiment analysis approaches," *Procedia Computer Science*, vol. 160, pp. 803–810, 2019, doi: 10.1016/j.procs.2019.11.007.
- [5] N. Saeed and L. Husamaldin, "Big data characteristics (V's) in industry," *Iraqi Journal of Industrial Research*, vol. 8, no. 1, pp. 1–9, Jun. 2021, doi: 10.53523/ijoirVol8I1ID52.

- [6] P. Sindhwad and F. Kazi, "Exploiting control device vulnerabilities: attacking cyber-physical water system," in *2022 32nd Conference of Open Innovations Association (FRUCT)*, Nov. 2022, vol. 2022-Novem, pp. 270–279. doi: 10.23919/FRUCT56874.2022.9953826.
- [7] M. A. Poltavtseva, D. P. Zegzhda, and M. O. Kalinin, "Big data management system security threat model," *Automatic Control and Computer Sciences*, vol. 53, no. 8, pp. 903–913, Dec. 2019, doi: 10.3103/S0146411619080261.
- [8] M. Khan and L. Ghafoor, "Adversarial machine learning in the context of network security: challenges and solutions," *Journal of Computational Intelligence and Robotics By The Science Brigade (Publishing) Group 51 Journal of Computational Intelligence and Robotics*, vol. 4, no. 1, pp. 51–63, 2024.
- [9] A. E. Cinà *et al.*, "Wild patterns reloaded: a survey of machine learning security against training data poisoning," *ACM Computing Surveys*, vol. 55, no. 13, 2023, doi: 10.1145/3585385.
- [10] A. Shafee and T. A. Awaad, "Privacy attacks against deep learning models and their countermeasures," *Journal of Systems Architecture*, vol. 114, 2021, doi: 10.1016/j.sysarc.2020.101940.
- [11] S. Wang, R. K. L. Ko, G. Bai, N. Dong, T. Choi, and Y. Zhang, "Evasion attack and defense on machine learning models in cyber-physical systems: a survey," *IEEE Communications Surveys and Tutorials*, vol. 26, no. 2, pp. 930–966, 2024, doi: 10.1109/COMST.2023.3344808.
- [12] N. A, H. J, S. P. S. Prakash, and K. Krinkin, "Class imbalance and concept drift invariant online botnet threat detection framework for heterogeneous IoT edge," *Computers and Security*, vol. 141, 2024, doi: 10.1016/j.cose.2024.103820.
- [13] E. D. Zamani, C. Smyth, S. Gupta, and D. Dennehy, "Artificial intelligence and big data analytics for supply chain resilience: a systematic literature review," *Annals of Operations Research*, vol. 327, no. 2, pp. 605–632, 2023, doi: 10.1007/s10479-022-04983-y.
- [14] M. N. I. Sarker, M. Wu, B. Chanthamith, and C. Ma, "Resilience through big data: natural disaster vulnerability context," in *Advances in Intelligent Systems and Computing*, 2020, vol. 1190 AISC, pp. 105–118. doi: 10.1007/978-3-030-49829-0\_8.
- [15] J. Ahmad and S. Baharom, "A systematic literature review of the test case prioritization technique for sequence of events," *International Journal of Applied Engineering Research*, vol. 12, no. 7, pp. 1389–1395, 2017.
- [16] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891.
- [17] K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. Siami Namin, "How social engineers use persuasion principles during phishing attacks," *Information and Computer Security*, vol. 29, no. 2, pp. 314–331, 2020, doi: 10.1108/ICS-07-2020-0113.
- [18] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: a recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, 2021, doi: 10.3389/fcomp.2021.563060.
- [19] D. Galinec and L. Luic, "Digital security perspectives and engagement for resilience in information-communication environment," in *Proceedings - 2019 3rd European Conference on Electrical Engineering and Computer Science, EECS 2019*, 2019, pp. 106–112. doi: 10.1109/EECS49779.2019.00032.
- [20] F. Abri, J. Zheng, A. S. Namin, and K. S. Jones, "Markov decision process for modeling social engineering attacks and finding optimal attack strategies," *IEEE Access*, vol. 10, pp. 109949–109968, 2022, doi: 10.1109/ACCESS.2022.3213711.
- [21] P. Zambrano, J. Torres, Á. Yáñez, A. Macas, and L. Tello-Oquendo, "Understanding cyberbullying as an information security attack-life cycle modeling," *Annales des Telecommunications/Annals of Telecommunications*, vol. 76, no. 3–4, pp. 235–253, 2021, doi: 10.1007/s12243-020-00785-0.
- [22] N. Tsinganos, I. Mavridis, and D. Gritzalis, "Utilizing convolutional neural networks and word embeddings for early-stage recognition of persuasion in chat-based social engineering attacks," *IEEE Access*, vol. 10, pp. 108517–108529, 2022, doi: 10.1109/ACCESS.2022.3213681.
- [23] Y. Aun, M. L. Gan, N. H. B. A. Wahab, and G. Hock Guan, "Social engineering attack classifications on social media using deep learning," *Computers, Materials and Continua*, vol. 74, no. 3, pp. 4917–4931, 2023, doi: 10.32604/cmc.2023.032373.
- [24] S. Sankhwar, D. Pandey, R. A. Khan, and S. N. Mohanty, "An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method," *Security and Privacy*, vol. 4, no. 1, 2021, doi: 10.1002/spy2.132.
- [25] P. A. Barraclough, G. Fehringer, and J. Woodward, "Intelligent cyber-phishing detection for online," *Computers and Security*, vol. 104, 2021, doi: 10.1016/j.cose.2020.102123.
- [26] A. Awasthi and N. Goel, "Phishing website prediction using base and ensemble classifier techniques with cross-validation," *Cybersecurity*, vol. 5, no. 1, 2022, doi: 10.1186/s42400-022-00126-9.
- [27] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, "Enterprise credential spear-phishing attack detection," *Computers and Electrical Engineering*, vol. 94, 2021, doi: 10.1016/j.compeleceng.2021.107363.
- [28] R. Hoffmann, "Markov model of cyber attack life cycle triggered by software vulnerability," *International Journal of Electronics and Telecommunications*, vol. 67, no. 1, pp. 35–41, 2021, doi: 10.24425/ijet.2021.135941.
- [29] Y. Roumani, "Patching zero-day vulnerabilities: an empirical analysis," *Journal of Cybersecurity*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab023.
- [30] M. Reveraert and T. Sauer, "Redefining insider threats: a distinction between insider hazards and insider threats," *Security Journal*, vol. 34, no. 4, pp. 755–775, 2021, doi: 10.1057/s41284-020-00259-x.
- [31] Y. Movahedi, M. Cukier, and I. Gashi, "Predicting the discovery pattern of publically known exploited vulnerabilities," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1181–1193, 2022, doi: 10.1109/TDSC.2020.3014872.
- [32] J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, "Improving vulnerability remediation through better exploit prediction," *Journal of Cybersecurity*, vol. 6, no. 1, 2020, doi: 10.1093/CYBSEC/TYAA015.
- [33] L. Allodi, M. Cremonini, F. Massacci, and W. Shim, "Measuring the accuracy of software vulnerability assessments: experiments with students and professionals," *Empirical Software Engineering*, vol. 25, no. 2, pp. 1063–1094, 2020, doi: 10.1007/s10664-019-09797-4.
- [34] K. Charmanas, N. Mittas, and L. Angelis, "Exploitation of vulnerabilities: a topic-based machine learning framework for explaining and predicting exploitation," *Information (Switzerland)*, vol. 14, no. 7, 2023, doi: 10.3390/info14070403.
- [35] I. B. Haimed, M. Albahar, and A. Alzubaidi, "Exploiting misconfiguration vulnerabilities in microsoft's azure active directory for privilege escalation attacks," *Future Internet*, vol. 15, no. 7, 2023, doi: 10.3390/fi15070226.
- [36] T. Yamauchi, Y. Akao, R. Yoshitani, Y. Nakamura, and M. Hashimoto, "Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes," *International Journal of Information Security*, vol. 20, no. 4, pp. 461–473, 2021, doi: 10.1007/s10207-020-00514-7.
- [37] J. Carrillo-Mondejar, H. Turtiainen, A. Costin, J. L. Martinez, and G. Suarez-Tangil, "HALE-IoT: hardening legacy Internet of Things devices by retrofitting defensive firmware modifications and implants," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8371–8394, 2023, doi: 10.1109/IJOT.2022.3224649.




- [38] M. Mehmood, R. Amin, M. M. A. Muslam, J. Xie, and H. Aldabbas, "Privilege escalation attack detection and mitigation in cloud using machine learning," *IEEE Access*, vol. 11, pp. 46561–46576, 2023, doi: 10.1109/ACCESS.2023.3273895.
- [39] J. Geng, J. Wang, Z. Fang, Y. Zhou, D. Wu, and W. Ge, "A survey of strategy-driven evasion methods for PE malware: transformation, concealment, and attack," *Computers and Security*, vol. 137, 2024, doi: 10.1016/j.cose.2023.103595.
- [40] S. Wasko *et al.*, "Using alternate reality games to find a needle in a haystack: an approach for testing insider threat detection methods," *Computers and Security*, vol. 107, 2021, doi: 10.1016/j.cose.2021.102314.
- [41] S. Yuan and X. Wu, "Deep learning for insider threat detection: review, challenges and opportunities," *Computers and Security*, vol. 104, 2021, doi: 10.1016/j.cose.2021.102221.
- [42] H. Hasan, B. Tork Ladani, and B. Zamani, "Maaker: a framework for detecting and defeating evasion techniques in Android malware," *Journal of Information Security and Applications*, vol. 78, 2023, doi: 10.1016/j.jisa.2023.103617.
- [43] H. Murray and D. Malone, "Adaptive password guessing: learning language, nationality and dataset source," *Annales des Telecommunications/Annals of Telecommunications*, vol. 78, no. 7–8, pp. 385–400, 2023, doi: 10.1007/s12243-023-00969-4.
- [44] I. Alkhwaja *et al.*, "Password cracking with brute force algorithm and dictionary attack using parallel programming," *Applied Sciences (Switzerland)*, vol. 13, no. 10, 2023, doi: 10.3390/app13105979.
- [45] A. Kanta, I. Coisel, and M. Scanlon, "A novel dictionary generation methodology for contextual-based password cracking," *IEEE Access*, vol. 10, pp. 59178–59188, 2022, doi: 10.1109/ACCESS.2022.3179701.
- [46] J. M. Esparza, "Understanding the credential theft lifecycle," *Computer Fraud and Security*, vol. 2019, no. 2, pp. 6–9, 2019, doi: 10.1016/S1361-3723(19)30018-1.
- [47] L. Wu, H. J. Cai, and H. Li, "SGX-UAM: a secure unified access management scheme with one time passwords via intel SGX," *IEEE Access*, vol. 9, pp. 38029–38042, 2021, doi: 10.1109/ACCESS.2021.3063770.
- [48] Y. Li, X. Yun, L. Fang, and C. Ge, "An efficient login authentication system against multiple attacks in mobile devices," *Symmetry*, vol. 13, no. 1, pp. 1–22, 2021, doi: 10.3390/sym13010125.
- [49] Z. Zhang, Y. Wang, and K. Yang, "Strong authentication without tamper-resistant hardware and application to federated identities," 2020. doi: 10.14722/ndss.2020.24462.
- [50] N. K. Blanchard, S. Kachanovich, T. Selker, and F. Waligorski, "Reflexive memory authenticator: a proposal for effortless renewable biometrics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11967 LNCS, pp. 104–121, 2020, doi: 10.1007/978-3-030-39749-4\_7.
- [51] R. M. Carnier, Y. Li, Y. Fujimoto, and J. Shikata, "Exact markov chain of random propagation of malware with network-level mitigation," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10933–10947, 2023, doi: 10.1109/JIOT.2023.3240421.
- [52] C. Gan, Q. Feng, X. Zhang, Z. Zhang, and Q. Zhu, "Dynamical propagation model of malware for cloud computing security," *IEEE Access*, vol. 8, pp. 20325–20333, 2020, doi: 10.1109/ACCESS.2020.2968916.
- [53] H. Rathore, A. Samavedhi, S. K. Sahay, and M. Sewak, "Robust malware detection models: learning from adversarial attacks and defenses," *Forensic Science International: Digital Investigation*, vol. 37, 2021, doi: 10.1016/j.fsidi.2021.301183.
- [54] H. M. Kim and K. H. Lee, "IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories," *Applied Sciences (Switzerland)*, vol. 12, no. 15, 2022, doi: 10.3390/app12157679.
- [55] R. Beg, R. K. Pateriya, and D. S. Tomar, "ACMFNN: a novel design of an augmented convolutional model for intelligent cross-domain malware localization via forensic neural networks," *IEEE Access*, vol. 11, pp. 87945–87957, 2023, doi: 10.1109/ACCESS.2023.3305274.
- [56] T. Shibahara, Y. Takata, M. Akiyama, T. Yagi, K. Hato, and M. Murata, "Evasive malicious website detection by leveraging redirection subgraph similarities," *IEICE Transactions on Information and Systems*, vol. E102D, no. 3, pp. 430–443, 2019, doi: 10.1587/transinf.2018FCP0007.
- [57] A. Javed, R. Ikwu, P. Burnap, L. Giommoni, and M. L. Williams, "Disrupting drive-by download networks on Twitter," *Social Network Analysis and Mining*, vol. 12, no. 1, 2022, doi: 10.1007/s13278-022-00944-2.
- [58] A. Javed, P. Burnap, M. L. Williams, and O. F. Rana, "Emotions behind Drive-by download propagation on twitter," *ACM Transactions on the Web*, vol. 14, no. 4, 2020, doi: 10.1145/3408894.
- [59] A. Javed, P. Burnap, and O. Rana, "Prediction of drive-by download attacks on twitter," *Information Processing and Management*, vol. 56, no. 3, pp. 1133–1145, 2019, doi: 10.1016/j.ipm.2018.02.003.
- [60] M. Alshehri and B. Panda, "A blockchain-encryption-based approach to protect fog federations from rogue nodes," *2019 3rd Cyber Security in Networking Conference, CSNet 2019*, pp. 6–13, 2019, doi: 10.1109/CSNet47905.2019.9108975.
- [61] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments," *IEEE Access*, vol. 7, pp. 80813–80828, 2019, doi: 10.1109/ACCESS.2019.2922196.
- [62] V. D. M. Rios, P. R. M. Inacio, D. Magoni, and M. M. Freire, "Detection and mitigation of low-rate denial-of-service attacks: a survey," *IEEE Access*, vol. 10, pp. 76648–76668, 2022, doi: 10.1109/ACCESS.2022.3191430.
- [63] Q. Wang, W. Tai, Y. Tang, H. Zhu, M. Zhang, and D. Zhou, "Coordinated defense of distributed denial of service attacks against the multi-area load frequency control services," *Energies*, vol. 12, no. 13, 2019, doi: 10.3390/en12132493.
- [64] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y. W. Chong, and Y. K. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller-a review," *IEEE Access*, vol. 8, pp. 143985–143995, 2020, doi: 10.1109/ACCESS.2020.3013998.
- [65] C. D. Phung, B. F. Silva, M. Nogueira, and S. Secci, "MPTCP robustness against large-scale man-in-the-middle attacks," *Computer Networks*, vol. 164, 2019, doi: 10.1016/j.comnet.2019.106896.
- [66] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, "Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, 2019, doi: 10.1109/TIFS.2018.2883177.
- [67] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, vol. 2019, 2019, doi: 10.1155/2019/4683982.
- [68] A. Lahmadi, A. Duque, N. Heraief, and J. Francq, "MitM attack detection in BLE networks using reconstruction and classification machine learning techniques," *Communications in Computer and Information Science*, vol. 1323, pp. 149–164, 2020, doi: 10.1007/978-3-030-65965-3\_10.
- [69] Q. Li, W. Li, J. Wang, and M. Cheng, "A SQL injection detection method based on adaptive deep forest," *IEEE Access*, vol. 7, pp. 145385–145394, 2019, doi: 10.1109/ACCESS.2019.2944951.
- [70] A. Chowdhary, K. Jha, and M. Zhao, "Generative Adversarial Network (GAN)-based autonomous penetration testing for web applications," *Sensors*, vol. 23, no. 18, 2023, doi: 10.3390/s23188014.
- [71] H. Sun, Y. Du, and Q. Li, "Deep learning-based detection technology for SQL injection research and implementation," *Applied Sciences (Switzerland)*, vol. 13, no. 16, 2023, doi: 10.3390/app13169466.






- [72] C. R. Pardomuan, A. Kurniawan, M. Y. Darus, M. A. M. Ariffin, and Y. Muliono, "Server-side cross-site scripting detection powered by HTML semantic parsing inspired by XSS auditor," *Pertanika Journal of Science and Technology*, vol. 31, no. 3, pp. 1353–1377, 2023, doi: 10.47836/pjst.31.3.14.
- [73] Q. Abu Al-Haija, "Cost-effective detection system of cross-site scripting attacks using hybrid learning approach," *Results in Engineering*, vol. 19, 2023, doi: 10.1016/j.rineng.2023.101266.
- [74] O. C. Abikoye, A. Abubakar, A. H. Dokoro, O. N. Akande, and A. A. Kayode, "A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm," *Eurasip Journal on Information Security*, vol. 2020, no. 1, 2020, doi: 10.1186/s13635-020-00113-y.
- [75] S. Kogan, T. J. Moskowitz, and M. Niessner, "Social media and financial news manipulation," *Review of Finance*, vol. 27, no. 4, pp. 1229–1268, 2023, doi: 10.1093/rof/rfac058.
- [76] M. Akram, A. Nasar, and A. Arshad-Ayaz, "A systematic review for netizens' response to the truth manipulation on social media," *Knowledge Management and E-Learning*, vol. 15, no. 2, pp. 322–342, 2023, doi: 10.34105/j.kmel.2023.15.018.
- [77] J. Wu, M. Cao, F. Chiclana, Y. Dong, and E. Herrera-Viedma, "An optimal feedback model to prevent manipulation behavior in consensus under social network group decision making," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 7, pp. 1750–1763, 2021, doi: 10.1109/TFUZZ.2020.2985331.
- [78] E. Yasasin, J. Prester, G. Wagner, and G. Schryen, "Forecasting IT security vulnerabilities-an empirical analysis," *Computers and Security*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101610.
- [79] C. Majdoubi, S. El Mendili, and Y. Gahi, "Data security patterns for critical big data systems," 2023, doi: 10.1109/CloudTech58737.2023.10366149.
- [80] G. Youssef, M. Guennoun, Z. Guennoun, and K. El-Khatib, "Encrypted processes for oblivious data retrieval," in *2011 International Conference for Internet Technology and Secured Transactions*, 2011, pp. 514–518.
- [81] Y. Gahi and I. E. Alaoui, "A Secure Multi-User Database-as-a-Service Approach for Cloud Computing Privacy," *Procedia Computer Science*, vol. 160, pp. 811–818, 2019, doi: 10.1016/j.procs.2019.11.006.

## BIOGRAPHIES OF AUTHORS






**Mrs. Majdoubi Chaymae**    is a Ph.D. student in Engineering Sciences Laboratory at the National School of Applied Sciences of Kenitra, Ibn Tofail University, Morocco. She is a state engineer with multidisciplinary programs, and a multiperspective vision. She's interested in data security in big data systems, contributing to data privacy and security. She recently zoomed in on mobile security to unlock new security and privacy challenges. She can be contacted at email: chaymae.majdoubi@uit.ac.ma.



**Prof. Dr. Gahi Youssef**    is an associate professor at the National School of Applied Sciences of Kenitra, Ibn Tofail University, Morocco. He received the M.Sc. and Ph.D. degrees in computer science from University Mohammed Vth in 2008 and 2013, respectively. His research topics focus on big data management, big data quality, security, and recommendation systems. Before starting his academic career in 2017, he worked for many international firms from 2008 to 2017 as a software engineer, solution architect, and IT consultant. He can be contacted at email: gahi.youssef@uit.ac.ma.



**Prof. Dr. El Mendili Saida**    is an assistant professor in computer science at Ibn Tofail University, Morocco. she obtained her state engineer diploma in computer engineering from Cadi Ayyad University, Morocco in 2010, and she gained her Ph.D. in computer science from Ibn Tofail University in 2020. Member of Engineering Science Laboratory in National Schools of Applied Sciences -Kenitra, technical program member and chair on several international conferences. Her research interests include artificial intelligence, big data analytics, machine learning, smart city. She can be contacted at email: elmendili.saida@uit.ac.ma.