

Safeguarding data privacy: strategies to counteract internal and external hacking threats

Hassan Jamal, Nasir Ahmed Algeelani, Najeeb Al-Sammarraie

Department of Computer and Information Technology, AL-Madinah International University, Kuala Lumpur, Malaysia

Article Info

Article history:

Received Jul 12, 2023

Revised Dec 07, 2023

Accepted Jan 05, 2024

Keywords:

Access controls

Data privacy

External hacking

Internal hacking

Intrusion detection systems

ABSTRACT

In the digital age, the protection of data privacy has become increasingly important. Hackers, whether internal or external to an organization, could cause significant damage by stealing sensitive data, causing financial loss, compromising the privacy of individuals, or damaging the organization's reputation. This scientific research aimed to make substantial contributions by emphasizing the importance of addressing both internal and external hacking threats to protect sensitive information. The main theme of their work revolved around building a multi-layered defense system that included technological solutions like firewalls, encryption, and intrusion detection systems. The specific goals of their design and development approach were to establish clear policies and procedures for data handling, access control, and incident response, as well as to enhance data privacy strategies to stay ahead of evolving hacking techniques. The authors also highlighted the significance of employee awareness and training programs, collaboration with cybersecurity experts, and staying up-to-date with regulatory requirements to create a robust data privacy framework.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Hassan Jamal

Department of Computer and Information Technology, AL-Madinah International University

Kuala Lumpur, Malaysia

Email: hassanaljammal@yahoo.com

1. INTRODUCTION

This research aims to explore strategies to counteract both internal and external hacking threats and safeguard data privacy. It investigates technical solutions such as encryption, firewalls, and intrusion detection systems, as well as organizational measures like employee training and access controls. The study highlights the importance of data privacy in today's digital age and the significant financial losses and compromised confidentiality that can result from hacking incidents. It emphasizes the need for effective measures to protect data privacy against internal and external threats. According to the Cost of Data Breach study, the average cost of a data breach is \$4.24 million [1]. These breaches can occur due to various reasons, including human error, system vulnerabilities, and malicious attacks by external or internal actors. The research uses a qualitative methodology, including semi-structured interviews with information technology (IT) security professionals and managers, to gather insights on the perceptions of technical and organizational solutions. Additionally, it conducts a literature review and analysis of relevant articles to provide a comprehensive understanding of data privacy protection strategies.

The results and discussions section summarizes key findings from the literature review, such as the effectiveness of machine learning techniques in detecting malware attacks and the need for strict access control policies to prevent insider threats. It also highlights the importance of comprehensive security measures to prevent social engineering attacks and data breaches [2]. In recent years, scholars have

highlighted the significance of adopting robust encryption techniques to secure sensitive data from unauthorized access [3]. Firewalls and intrusion detection systems have also proven instrumental in detecting and mitigating external hacking attempts [4]. Moreover, organizational measures, including employee training programs and strict access controls, play a pivotal role in mitigating internal vulnerabilities and promoting a culture of data privacy [5]. This research aims to explore diverse methodologies for safeguarding data privacy against both internal and external hacking attempts. By investigating technical solutions such as encryption, firewalls, and intrusion detection systems, alongside organizational measures like employee training and access controls, this study seeks to provide comprehensive insights into enhancing data privacy protection [6], [7].

The research concludes by providing recommendations for effective data privacy protection. These recommendations include implementing centralized systems to address security risks, limiting access to minimize data exposure, using strong passwords and multi-factor authentication, and employing email filtering and antivirus software. The adoption of zero trust security and the promotion of a culture of awareness and training are also emphasized.

Overall, this research contributes to the development of comprehensive strategies to safeguard data privacy and counteract internal and external hacking threats. It provides insights into technical and organizational measures that organizations can implement to protect sensitive information, maintain data integrity and confidentiality, and mitigate risks associated with data breaches.

Variables definition

- Data

Data is information collected or generated to infer biological phenomena, act as empirical evidence, and drive innovation. It can be used as plural or singular subjects in electronic computing and can be converted into binary digital form plural subjects in digital computing and can also be converted into binary digital form [8]. Data may be characterized as a methodical documentation of a specific measure. It encompasses the assorted values of said measure unified within a group. It constitutes an assemblage of information and numerical data to be employed for a precise intention, such as a survey or examination. When arranged in a structured manner, it can be referred to as information. The origin of data (primary data, secondary data) also holds significance.

- Privacy

Privacy, a complex concept with over 100 years of research, remains fragmented with inconsistent concepts, definitions, and relationships. It can mean the right to control information about oneself or individual isolation. The organization for economic cooperation and development (OECD) principles provide high-level privacy standards, but legislation varies by geography and domain, making it difficult to create a single privacy policy covering all personal information. Privacy is a crucial security principle in IoT, ensuring that users can only control their data and not share it with others. It is essential for society's freedom and prosperity, as it prevents the disclosure of sensitive information. Privacy is defined in various forms, including big data privacy, which focuses on preventing the disclosure of sensitive information [9].

- Data-privacy

Data privacy protects individual sensor observations from fusion centers, ensuring they cannot infer original observations. It involves obfuscating raw data while extracting statistical information. Data privacy is an expanding sub-field of data management aimed at handling sensitive data without compromising privacy [10].

- Protect

Means the noble endeavor of preserving and upholding the present condition or intrinsic nature of a given entity, be it an idea, a value, or a tangible object, through the provision of monetary or legal assurances or guarantees. This multifaceted concept entails not only shielding against potential perils or setbacks of a financial nature that may emerge in the days to come, but also fostering and shielding from any potential encroachment or restriction that might impede the full realization of its potential. By offering a robust shield against the vicissitudes of time and circumstance, protection acts as a guardian, safeguarding the essence and integrity of that which is held dear, ensuring its perpetual existence and unimpeded growth [6], [11].

- Hacking

Hacking, which was originally conceived as a creative endeavor in the realm of computer programming, is frequently misconstrued within the network culture, leading to a multitude of misunderstandings and misconceptions. This multifaceted activity often encompasses the intricate process of re-engineering systems, wherein individual's adept in the art of hacking skillfully manipulates and modify existing frameworks to suit their needs. Furthermore, hacking involves the ingenuity of transforming principles derived from ancient traditions, seamlessly blending the wisdom of the past with the innovation of the present. However, it is important to note that this intricate pursuit is not without its consequences, as it

has the potential to cause disappointment and loss, underscoring the inherent risks associated with this unorthodox practice [12].

- Internal-hacking

An internal attack is a sophisticated computer attack used by highly-skilled employees or technical users to disrupt operations or exploit assets. It can be initiated by a malicious node, which becomes active data route element. Networks are more vulnerable to internal attacks due to difficulty in detecting them. Internal hacking occurs when data is hacked in static mode [13].

- External-hacking

Policies aimed at alleviating vulnerabilities within information systems predominantly concentrate on safeguarding against security threats pertaining to the operational software, such as those originating from external hacking endeavors and unauthorized access attempts. Conversely, the focus on mitigating insider threats, such as the nefarious act of developers inserting malicious code into the system, tends to be comparatively less pronounced. External threats, on the other hand, pertain to the malicious activities of individuals who exploit existing vulnerabilities to gain unauthorized access to the system, encompassing a wide array of activities ranging from the surreptitious installation of malware to perpetrating distributed denial-of-service (DDoS) Attacks. [14].

- Data-privacy internal hacking

Data privacy is crucial for protecting data from external and internal threats, determining data sharing, and regulations. A personal data breach involves accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of data. Employees can also cause breaches, either accidentally or intentionally [15].

- Data-privacy external-hacking

Information security is frequently portrayed as a looming menace that originates from external forces, however, it is crucial to recognize that the challenges arising from the ever-growing reliance on information are not solely attributable to external threats, but can also be traced back to internal mechanisms. While it is true that external breaches of data can manifest themselves in a multitude of forms, ranging from malevolent hackers seeking to exploit vulnerabilities, to online institutions that may inadvertently mishandle sensitive information, to even governmental bodies that may be motivated by a variety of factors, it is vital to acknowledge that these occurrences are not the sole source of concern when it comes to safeguarding information. Rather, it is the very intricate and intricate internal processes that are interwoven within an organization's information infrastructure that can pose significant risks, as they can potentially expose sensitive data to unauthorized access or manipulation [16].

- Data confidentiality

The concept of protecting sensitive information from unauthorized access or disclosure, commonly referred to as data security, is of paramount importance within the realm of data privacy. This fundamental aspect ensures that data, whether it be personal or business-related, can solely be accessed by individuals or systems that have been granted the necessary authorization. The significance of data security lies in its ability to safeguard valuable information from falling into the wrong hands, thereby minimizing the potential risks and consequences associated with unauthorized data breaches or leaks [17].

- Data integrity

Referring to the accuracy, completeness, and consistency of data throughout its entire lifecycle is of utmost significance. This entails the crucial task of guaranteeing that data remains unaltered and untampered with by individuals or systems who lack the necessary authorization. The assurance of data integrity plays a pivotal role in upholding the sanctity and reliability of information, safeguarding it against any unauthorized modifications or tampering that may occur [18].

- Data availability

The concept of data availability pertains to the capability of retrieving and utilizing data as and when required. This encompasses the crucial task of safeguarding data from any potential loss or destruction caused by system malfunctions, unforeseen circumstances, or even natural calamities. The significance of ensuring data availability cannot be overstated, as any interruption in accessing data can have severe consequences for businesses and organizations, hindering their operations, decision-making processes, and overall productivity. Therefore, it becomes imperative to establish robust measures and protocols to mitigate the risks associated with data unavailability [19].

- Data minimization

Referring to the practice of gathering and retaining solely the absolute minimum quantity of information required for a precise objective, data minimization encompasses the act of diminishing the likelihood of divulging sensitive data to unauthorized entities or systems. By implementing this principle, organizations aim to adhere to a meticulous approach that ensures the strict limitation of data collection and storage, thereby mitigating the potential risks associated with unauthorized access or disclosure of confidential information. By adhering to this approach, entities demonstrate their commitment to

safeguarding the privacy and security of individuals' personal data, while simultaneously fostering an environment of trust and accountability within their operations [20].

- User consent

Acquiring explicit and well-informed consent from users prior to the collection or utilization of their personal information is commonly referred to as the practice of consent. This practice encompasses providing users with the ability to exercise control over their data, thereby ensuring that their privacy preferences are duly acknowledged and adhered to. By seeking consent, organizations demonstrate their commitment to respecting the autonomy and agency of individuals in determining the fate of their personal data, thus fostering trust and transparency in the realm of data privacy [21].

- Social engineering

Psychological manipulation, which is commonly referred to as the utilization of strategic tactics aimed at deceiving individuals into revealing confidential information or engaging in activities that jeopardize security, entails the exploitation of human vulnerabilities as opposed to technical ones. This intricate process revolves around the cunning manipulation of the human psyche, wherein individuals are coerced into sharing sensitive data or executing actions that may have disastrous consequences for both personal and organizational security measures. By leveraging the inherent weaknesses and susceptibilities of the human mind, this artful technique capitalizes on emotional triggers, cognitive biases, and social engineering strategies to circumvent traditional security protocols and gain unauthorized access to valuable information [5].

- Phishing

The employment of deceptive electronic mails or internet sites with the intention of deceiving individuals into divulging confidential data including passcodes, financial card digits, or government-issued identity numbers is an exceedingly prevalent modus operandi employed by cybercriminals. This method, commonly referred to as a cyber attack, entails the perpetrators employing fraudulent means to manipulate unsuspecting internet users into revealing sensitive personal information, thereby enabling the assailants to exploit this data for their nefarious purposes. It is imperative to remain vigilant in order to safeguard oneself against falling victim to such fraudulent activities [22].

- Malware

Malicious software, often referred to as malware, is specifically crafted to breach the security of computer systems or networks with the intention of inducing harm, retrieving sensitive information, or engaging in covert surveillance. This encompassing term encompasses a variety of insidious digital threats, such as viruses, worms, Trojans, and spyware, each with their own unique methods and objectives. These sophisticated programs are designed to exploit vulnerabilities within computer systems and networks, leveraging their access to compromise data integrity, disrupt operations, or covertly monitor user activities [23].

- Insider threat

The term "insider threat" pertains to the potential danger that arises from individuals who are affiliated with an organization and possess the ability to access classified data or computer networks, and could potentially exploit this access with the intent to cause damage, whether intentional or unintentional. This category encompasses both present and past employees, as well as contracted personnel and collaborators who are associated with the organization. The insider threat is a multifaceted issue that necessitates comprehensive attention and mitigation strategies in order to safeguard against potential risks and protect the integrity of sensitive information and systems [24].

- Cyber espionage

Cyber espionage, commonly known as the utilization of cyber attacks to acquire illicit entry into classified information or intellectual property owned by governmental bodies, institutions, or individuals, is a prevalent phenomenon in the digital realm. This clandestine operation is frequently linked to the involvement of nation-state actors, wherein governments engage in covert activities to obtain confidential data for their own strategic interests. The unauthorized access to sensitive information or intellectual property through cyber espionage poses significant threats to the security and privacy of governments, organizations, and individuals, and thus necessitates robust cybersecurity measures to mitigate these risks effectively [15].

- Awareness

The awareness of data privacy is of utmost importance. As it serves a pivotal function in safeguarding and fortifying the security of both sensitive and confidential data. Adhering strictly to established security protocols and effectively thwarting any potential breaches that may arise and could potentially expose sensitive information to a significant risk that could compromise both the integrity and privacy of said information [25].

- Training and education

Training programs play a pivotal role in amplifying the knowledge base and honing the skills of employees, consequently leading to a substantial decrease in security incidents, thereby fostering and nurturing a culture that is deeply rooted in awareness and consciousness [5]. Effective training programs have the ability to not only enhance the overall security awareness within an organization, but also to foster a

culture that places a high importance on the safety and protection of its employees and sensitive information. By implementing comprehensive training initiatives, companies can effectively equip their workforce with the necessary knowledge and skills to identify and report any potentially suspicious activities, thereby fostering a more proactive and vigilant approach towards security. Through these training programs, employees are empowered to actively contribute to the overall security posture of the organization, creating a collaborative and unified front against potential threats.

- Technology and infrastructure

Data security is heavily reliant on a myriad of diverse and extensive factors. But, certainly not limited to state-of-the-art and groundbreaking technology that is specifically formulated and engineered with the explicit purpose of safeguarding and protecting sensitive and confidential information from any form of unauthorized access or breach. A robust and resilient infrastructure that serves as the fundamental bedrock and backbone of the comprehensive security framework, employing cutting-edge and advanced encryption techniques that effectively render any and all data incomprehensible, indecipherable, and impervious to any individual lacking the requisite decryption keys, consistent and punctual system updates that diligently and promptly address and mitigate emerging threats and vulnerabilities, meticulous and conscientious maintenance practices that ensure the seamless and optimal functionality and operation of the implemented security measures, and lastly, but certainly not least, an impregnable and fortified network infrastructure that serves as an impenetrable and formidable barrier, effectively warding off and thwarting any malicious and unauthorized intrusions [11].

- Risk management

Risk management encompasses the process of implementing a meticulously designed framework that is aimed at effectively identifying, assessing, and mitigating potential security risks. This encompassing process further entails conducting regular and comprehensive assessments, which enable organizations to gain a holistic understanding of their security posture and identify areas that require immediate attention. Furthermore, risk management involves the development of a well-thought-out incident response plan, which provides organizations with a strategic blueprint to proactively address any security incidents that may arise, thereby minimizing the potential impact and ensuring the continuity of operations [23].

- Organizational culture

Organizational culture plays a crucial role in promoting data privacy and security. Management commitment, employee commitment, and open communication channels are essential for fostering security awareness and reporting. Effective policies and procedures are crucial to protect against social engineering attacks and maintain data confidentiality [26].

Relations among variables

- Relation between data-privacy and internal-hacking

Current network security technology cannot resist hacker attacks, but internal disclosure and staff supervision can lead to personal data leakage. To prevent data leakage during outbreaks, special encryption systems and strict access mechanisms should be implemented. Encrypted data storage and computations, using cryptographic algorithms like Enigma6 and homomorphic encryption, can help maintain data privacy and prevent external hacking. Combining these approaches with distributed repositories offers a solution to resiliency against attacks and address data privacy concerns [27].

- Relation between data-privacy and external-hacking

Information security is often framed as an external threat. But, the problems created by increased dependency on information are not external threats but internal processes. Data security has complexities, including external cyberattacks, detection difficulties, and C-suite unfamiliarity [16].

- Some ways of data-privacy internal-hacking

i) Internal data leakage: Data leakage occurs from deliberate actions or accidental mistakes [28].
 ii) Malware: is malicious software designed to compromise a system, steal data, modify core functions, and track activities. Factors include outdated operating systems, unprotected links, and pirated software.
 iii) Physical security threats: involve direct access to sensitive information on devices, often underestimated compared to technical threats [29].
 iv) Compliance with data privacy regulations is extremely challenging with current data processing systems. Data privacy regulations are challenging due to their natural language and outdated systems. Compliance is also challenging due to multiple copies and lack of systematic record-keeping [30].

- Some ways of data-privacy external-hacking

i) DDoS attacks cause network overload and traffic congestion through targeted machines. ii) Session hijacking is a man-in-the-middle attack where an attacker replaces an IP address. iii) Drive-by attack spreads malware through insecure websites, installing on visitors' computers or redirecting them to hacked websites. iv) Passwords are vulnerable to hacking, gaining access through network sniffing, social

engineering, and physical examination. v) Shadow IT refers to unauthorized third-party software, applications, or internet services in the workplace, often hard to trace. Employees use these applications for efficiency, ease of use, and user-friendliness, creating a blind spot in cybersecurity strategies. Potential vulnerabilities can lead to data leaks, security breaches, and non-compliance with data protection legislation, resulting in steep fines [31]. vi) Social engineering (e.g., phishing) attacks increasingly sophisticated, Target failed to protect sensitive data, segregate networks, and harden systems.

2. METHOD

In this study, a qualitative data method was employed to address the research questions and hypotheses. The quantitative data were collected through a semi-structured interviews of some IT security professionals and managers to identify their perceptions of the technical and organizational solutions. The structured interview included questions related to the types of data privacy protections that are in place, the effectiveness of these protections, and any experiences with data breaches or cyber attacks. Moreover, the qualitative data were collected through the data that were gathered by scanning the internet and databases for related articles to data privacy and security. The results were used to answer the research main question and provide recommendations for effective data privacy protection to look for the available ways of protecting data privacy against internal or external hacking.

Figure 1 is a diagram of the steps of a research methodology focused on data privacy. The diagram is divided into four phases:

- a. Literature Analysis: i) Wide scan for recent articles that are related to research variables and relations among them. ii) Describe clearly the data-privacy, its boundaries, and the violation of data-privacy and internal and external hacking threats. iii) Define properly the required data type to be analyzed. iv) Define and assign the potential data sources. v) Confirm data sources best which will participate.
- b. Interviews: Collect main dimensions, concerning internal and external hacking threats.
- c. Data Analysis: i) A model an excel sheet was designed for data analysis. ii) Collect ways of protecting data from external hacking and reformulate data prior it is exposed. iii) Initial analysis of gathered data during interviews against research objectives. iv) All gathered information was entered into the built model, and reviewed. v) Gathered data were examined and analyzed.
- d. Report Writing: Results and Recommendations.

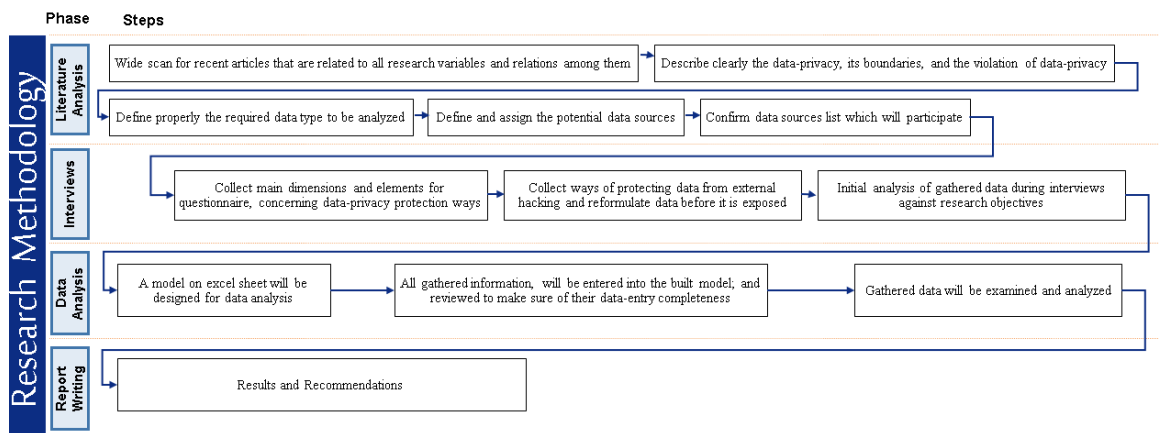


Figure 1. Research methodology

2. RESULTS AND DISCUSSIONS

The subsequent elucidation furnishes a comprehensive overview of the comprehensive assessments of the scholarly writings and empirical examinations undertaken by an assortment of authors within the realm of data security and privacy. These investigations delved into diverse facets of safeguarding data and proffered revelations pertaining to the efficacy of distinct techniques and methodologies. In light of this, it is evident that the aforementioned studies have contributed significantly to the understanding of data protection and have shed light on the viability and efficiency of specific approaches employed in this domain.

In their study [32], the authors conducted a literature review and experimental analysis to explore the taxonomy of internal attacks in wireless sensor networks. They employed machine learning techniques

and demonstrated that these techniques can effectively detect and prevent malware attacks. The proposed model achieved a high accuracy rate in detecting different types of malware.

Another study [24] focused on the coming of cyber espionage norms. The authors conducted a literature review and experimental analysis to develop an approach for detecting cyber espionage attacks. The proposed approach was found to be effective in detecting such attacks with a high accuracy rate. It was considered as a valuable tool for protecting data integrity against cyber espionage attacks.

The impact of leadership styles on information security compliance behavior was investigated in a systematic literature review [25]. The review highlighted the significant threat posed by insiders to data integrity and confidentiality. To mitigate this threat, organizations were advised to implement strict access control policies and monitor employee behavior closely.

The challenges of the digital age for privacy and personal data protection were explored in another literature review [1]. The review emphasized the necessity of effective cybersecurity risk assessment models to safeguard data integrity against cyber attacks. Several models were identified as suitable for assessing cybersecurity risks in critical infrastructure.

Social engineering attacks and their impact on data security and patient privacy were the focus of a literature review and case study analysis [33]. The study revealed that social engineering attacks pose a significant threat to data confidentiality and can result in data breaches. To counter such attacks, organizations were advised to implement comprehensive security measures.

Lastly, a literature review and experimental analysis investigated data privacy in the age of digital transformation [7]. The study proposed a technique for effectively detecting and preventing phishing attacks. The technique demonstrated a high accuracy rate in protecting data integrity against phishing attacks.

3.1. Some ways to protect the data-privacy against internal-hacking

a) Through what centralized systems face security risks, legal exposure, and internal hacking attacks. b) Limiting access to minimize data access, use The principle of least privilege (PoLP) , and manage permissions effectively [34]. c) Be aware of all software usage in your organization for effective internal security and consistent updates. d) Implement a company-wide password manager and policies to protect against Kerberoasting attacks and ensure strong passwords. e) Use multi-factor authentication for employees' accounts, as weak passwords can be easily accessed by hackers, ensuring security and preventing compromises in online services. f) Existence of a layer of email filtering. Microsoft Office 365 and Google Workspace offer native email filtering, third-party products control. g) Implement better antivirus/endpoint detection and response (EDR) software: Improve antivirus/EDR software reliability in small businesses through central administration. h) Provide zero trust remote network access: Distributed workforce requires zero trust security using cloud-based technologies like Secure Access Service Edge (SASE) and Social Democratic Party (SDP) for restricted remote privileges. i) Give internal users access to the minimum needed resources: The Principle of Least Privilege ensures users have access only for their job, including database software, limiting access to necessary fields and encrypted fields. j) Conduct internal security awareness training for employees and contractors, focusing on phishing, business email compromise (BEC), and social engineering, to protect against potential breaches [35].

3.2. Some ways to protect the data-privacy against external-hacking

a) Get expert help. b) Regularly review bank accounts, credit reports for potential information theft. c) Be cautious of scams, fake emails, and government messages. d) Avoid oversharing on social media to protect personal information. e) Use strong, unique online passwords with at least 12 characters. f) Ensure device security in industrial control systems, as reliance on internet protocols increases vulnerability to cyber threats and the internet of things. g) Firewalls are essential cybersecurity accessories for industrial PCs, control systems, and sewage systems. h) Transfer control protocol enforces uni-directional data transmission between users utilizing function codes for control. i) Master and slave simulator configurations extract slave information [36]. Organizations must secure personal data by collecting only required information [31].

These findings collectively emphasize the importance of adopting a multi-faceted approach to safeguard data privacy and counteract hacking threats. The results highlight the significance of strict access control policies, robust detection mechanisms, employee training, and comprehensive security measures. By integrating these findings into organizations' cybersecurity strategies, they can enhance their ability to protect data integrity, mitigate risks, and respond effectively to hacking threats. Despite the undeniable provision of significant and valuable insights by these aforementioned studies, it is of utmost importance to acknowledge and emphasize that there is an absolute necessity to comprehend and appreciate the reality that further extensive research and experimentation are fundamentally essential and indispensable in order to consistently and continuously advance and progress the strategies employed for the purpose of safeguarding and preserving the confidentiality and integrity of data amidst the incessantly evolving and perpetually shifting

landscape of hacking threats, which incessantly pose an ongoing and persistent challenge that must be perpetually addressed and overcome in order to maintain the sanctity and security of sensitive information.

3. CONCLUSION

In conclusion, safeguarding data privacy and countering internal and external hacking threats require a comprehensive approach that encompasses technological defenses, policies, employee training, and incident response plans. The proliferation of high-profile data breaches and hacking incidents serves as a stark reminder of the need for organizations to prioritize data privacy and implement proactive measures. By thoroughly reviewing the relevant literature, this research has highlighted the importance of addressing both internal and external hacking threats to protect sensitive information. The research has emphasized the significance of building a multi-layered defense system that includes robust technological solutions, such as firewalls, encryption, and intrusion detection systems. However, technology alone is not enough. Organizations must also establish clear policies and procedures for data handling, access control, and incident response. Employee awareness and training programs play a crucial role in mitigating the risks associated with internal breaches, as well as phishing and social engineering attacks. Moreover, the research has identified the need for organizations to continually update and enhance their data privacy strategies to stay ahead of evolving hacking techniques. This involves staying informed about the latest cyber security trends, conducting regular security assessments, and implementing proactive measures to identify and address vulnerabilities in systems and networks. Collaboration with cyber security experts and staying up-to-date with regulatory requirements also contribute to a robust data privacy framework. By implementing the proposed strategies, organizations can enhance their data privacy practices, mitigate the risks of data breaches, and protect the integrity and confidentiality of sensitive information.




REFERENCES

- [1] R. P. Romansky and I. S. Noninska, "Challenges of the digital age for privacy and personal data protection," *Mathematical Biosciences and Engineering*, vol. 17, no. 5, pp. 5288–5303, 2020, doi: 10.3934/mbe.2020286.
- [2] M. Tripathi and A. Mukhopadhyay, "Financial loss due to a data privacy breach: an empirical analysis," *Journal of Organizational Computing and Electronic Commerce*, vol. 30, no. 4, pp. 381–400, Sep. 2020, doi: 10.1080/10919392.2020.1818521.
- [3] N. Hemalatha, A. Jenis, A. Cecil Donald, and L. Arockiam, "A comparative analysis of encryption techniques and data security issues in cloud computing," *International Journal of Computer Applications*, vol. 96, no. 16, pp. 1–6, Jun. 2014, doi: 10.5120/16875-6873.
- [4] H. Cavusoglu, S. Raghunathan, and H. Cavusoglu, "Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems," *Information Systems Research*, vol. 20, no. 2, pp. 198–217, Jun. 2009, doi: 10.1287/isre.1080.0180.
- [5] F. Nel and L. Drevin, "Key elements of an information security culture in organisations," *Information & Computer Security*, vol. 27, no. 2, pp. 146–164, Jun. 2019, doi: 10.1108/ics-12-2016-0095.
- [6] C. Lambrinouidakis, "The general data protection regulation (GDPR) era: ten steps for compliance of data processors and data controllers," in *Lecture Notes in Computer Science*, Springer International Publishing, 2018, pp. 3–8. doi: 10.1007/978-3-319-98385-1_1.
- [7] H. S. A. Ahmed, "Data privacy in the age of digital transformation," PEBC Insights. Accessed: Jun. 24, 2023. [Online]. Available: <https://insights.pecb.com/data-privacy-age-digital-transformation/>
- [8] A. F. Wise, "Educating data scientists and data literate citizens for a new generation of data," *Journal of the Learning Sciences*, vol. 29, no. 1, pp. 165–181, Dec. 2019, doi: 10.1080/10508406.2019.1705678.
- [9] Smith, Dinev, and Xu, "Information privacy research: an interdisciplinary review," *MIS Quarterly*, vol. 35, no. 4, p. 989, 2011, doi: 10.2307/41409970.
- [10] M. Sun and W. P. Tay, "On the relationship between inference and data privacy in decentralized IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 852–866, 2020, doi: 10.1109/tifs.2019.2929446.
- [11] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 International Conference on Computer Science and Electronics Engineering*, IEEE, Mar. 2012, doi: 10.1109/iccsee.2012.193.
- [12] J. M. Reagle, *Hacking life: systematized living and its discontents*. 2019.
- [13] T. Yuvaraja and R. S. Sabeenian, "Dual tree complex wavelet transform-based image security using steganography," *Applied Mathematics & Information Sciences*, vol. 13, no. 2, pp. 215–222, Mar. 2019, doi: 10.18576/amis/130209.
- [14] S. Laxman, "Tutorial on the state of data privacy," *Proceedings of the 17th International Conference on Management of Data*, 2011.
- [15] M. R. Ahmed, X. Huang, and D. Sharma, "A taxonomy of internal attacks in wireless sensor network," *World Academy of Science, Engineering and Technology*, vol. 62, pp. 427–430, 2012.
- [16] C. Laybats and L. Tredinnick, "Information security," *Business Information Review*, vol. 33, no. 2, pp. 76–80, Jun. 2016, doi: 10.1177/0266382116653061.
- [17] G. Dhillon and J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Communications of the ACM*, vol. 43, no. 7, pp. 125–128, Jul. 2000, doi: 10.1145/341852.341877.
- [18] M. Yang, "Information security risk management model for big data," *Advances in Multimedia*, vol. 2022, pp. 1–10, Aug. 2022, doi: 10.1155/2022/3383251.
- [19] Y. Liu, T. Zhang, X. Jin, and X. Cheng, "Personal privacy protection in the era of big data," *Jisuanji Yanjiu yu Fazhan/Computer Research and Development*, vol. 52, no. 1, pp. 229–247, 2015, doi: 10.7544/issn1000-1239.2015.20131340.
- [20] A. Acquisti, "Privacy in electronic commerce and the economics of immediate gratification," *Proceedings of the ACM Conference on Electronic Commerce*, vol. 5, pp. 21–29, 2004, doi: 10.1145/988772.988777.
- [21] M. Dunn Cavelty, *Cybersecurity in Switzerland*. Springer International Publishing, 2014, doi: 10.1007/978-3-319-10620-5.
- [22] N. Valiyaveedu, S. Jamal, R. Reju, V. Murali, and N. K. M., "Survey and analysis on AI based phishing detection techniques," in *2021 International Conference on Communication, Control and Information Sciences (ICCCIS)*, IEEE, Jun. 2021, doi:




- 10.1109/iccisc52257.2021.9484929.
- [23] Imperva, "Data security," Imperva. Accessed: Jun. 24, 2023. [Online]. Available: <https://www.imperva.com/learn/data-security/data-security>
- [24] M. J. Culnan and R. J. Bies, "Consumer privacy: balancing economic and justice considerations," *Journal of Social Issues*, vol. 59, no. 2, pp. 323–342, Apr. 2003, doi: 10.1111/1540-4560.00067.
- [25] N. Humaidi and V. Balakrishnan, "Leadership styles and information security compliance behavior: the mediator effect of information security awareness," *International Journal of Information and Education Technology*, vol. 5, no. 4, pp. 311–318, 2015, doi: 10.7763/ijiet.2015.v5.522.
- [26] C. Sekhar Bhusal, "Systematic review on social engineering: hacking by manipulating humans," *Journal of Information Security*, vol. 12, no. 01, pp. 104–114, 2021, doi: 10.4236/jis.2021.121005.
- [27] T. Hardjono and A. S. Pentland, "Preserving data privacy in the IoT world," *Massachusetts Institute of Technology*, pp. 1–8, 2016.
- [28] L. Cheng, F. Liu, and D. (Daphne) Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *WIREs Data Mining and Knowledge Discovery*, vol. 7, no. 5, Sep. 2017, doi: 10.1002/widm.1211.
- [29] A. Johar, "Internet security 101 Six ways hackers can attack you and how to stay safe," *TheEconomicTimes*. Accessed: Oct. 30, 2017. [Online]. Available: <https://economictimes.indiatimes.com/tech/internet/internet-security-101-six-ways-hackers-can-attack-you-and-how-to-stay-safe/printarticle/61342742.cms>
- [30] L. Wang *et al.*, "Data capsule: a new paradigm for automatic compliance with data privacy regulations," in *Lecture Notes in Computer Science*, Springer International Publishing, 2019, pp. 3–23. doi: 10.1007/978-3-030-33752-0_1.
- [31] M. Adams, "Big data and individual privacy in the age of the internet of things," *Technology Innovation Management Review*, vol. 7, no. 4, pp. 12–24, Apr. 2017, doi: 10.22215/timreview/1067.
- [32] M. Libicki, "The coming of cyber espionage norms," in *2017 9th International Conference on Cyber Conflict (CyCon)*, IEEE, May 2017. doi: 10.23919/cycon.2017.8240325.
- [33] J. Whitfill, "Data security and patient privacy," in *Practical Imaging Informatics*, Springer US, 2021, pp. 119–130. doi: 10.1007/978-1-0716-1756-4_8.
- [34] Wordstream, "Customer data privacy: 10 non-negotiable best practices to protect your business," Wordstream. Accessed: Jun. 24, 2023. [Online]. Available: <https://www.wordstream.com/blog/ws/2022/11/22/customer-data-privacy>
- [35] FORTIS, "21 ways to protect your network from internal threats." Accessed: Jun. 24, 2023. [Online]. Available: <https://fortistelecom.net/cyber-security/protect-network-internal-threats/>
- [36] A. Mungekar, Y. Solanki, and R. Swarnalatha, "Augmentation of a SCADA based firewall against foreign hacking devices," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, p. 1359, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1359-1366.

BIOGRAPHIES OF AUTHORS






Hassan Jamal    is a highly accomplished individual and result-driven and seasoned top level management professional possessing 29 years of insightful experience in delivering large scale strategy projects, shaping IT Initiatives and driving program management initiatives as per organizational requirements. Accomplished his master in business management from MEDIU in Malaysia, on 2016, and the bachelor degree in computer sciens from M'utah university, in Jordan, on 1994. He is oriented management consulting professional (with Big4 experience), excel in service projects delivery offering more than two decades of diverse experience in different capacities primarily in the areas of strategic planning and execution, corporate governance, PMO governance, project planning, project and program management, business analysis, business process management, e-government and e-commerce services, IT services, ERP implementation. He can be contacted at email: hassanaljammal@yahoo.com



Dr. Nasir Ahmed Algeelani    is currently a Senior Lecturer in the Computer Science Department at Al-Madinah International University (MEDIU), Kuala Lumpur, Malaysia. Previously he worked as Lecturer at Industrial Technical Institute (ITI) from 2000 to 2010. Dr. Nasir Ahmed Algeelani received the B.E. degree in electrical power system from University of Aden, Yemen, Aden, in 1997, the M.E. degree in electrical power system engineering from University Technology Malaysia in 2009 and the Ph.D. degree in high voltage engineering from University Technology Malaysia in 2014. He conducted a postdoctorate at high voltage engineering department at University Technology Malaysia (2014-2016). He has published as authored and co-authored more than 30 papers in various technical journals and conference proceedings. His research interests include high-voltage instrumentation, partial discharge, detection and warning systems and condition monitoring of high-power equipment. He can be contacted at email: nasir.ahmed@mediu.edu.my



Dr. Najeeb Abbas Al-Sammaraie    joined MEDIU in SEPT.2012 as a lecturer in Faculty of computer and Information Technology. He completed my M.Sc. from North Staffordshire University in UK, worked in computer center in Iraq for more than 15 years as a Software manager. After completed Ph.D. start working in private University in Iraq. Having over 15 years' experience as senior lecturer, also as a Dean of Private University College, Head of Computer Department for more than 5 Years. Since SEPT.2012 in MEDIU had many responsibility and academic positions such as Dean of Library Deanship, Dean of ICT Faculty. Taught many Bachelor and Mater subjects, and still teaching each semester in the area of E-Services. Also working as an Asso Prof. to supervise many Master and Ph.D. students. Issues many research papers and join many international conferences. He can be contacted at email: dr.najeeb@mediu.edu.my