Exploring Data Wiping Practices in the Royal Malaysian Air Force (RMAF) HQ

Syed Nasir Alsagoff Bin Syed Zakaria(✉), Kuan Fook Chao(✉), and Zuraini Zainol(✉)

Department of Computer Science, Faculty of Defense Science and Technology,
Universiti Pertahanan Nasional Malaysia, Kem Sungai Besi, 57000 Kuala Lumpur, Malaysia
{syednasir,3221735,zuraini}@upnm.edu.my

Abstract. Data wiping is a very important part of cybersecurity. It is the act of deleting data so that it cannot be recovered. The Royal Malaysian Air Force (RMAF) as part of the Malaysian Armed Forces (MAF) has also recognized the importance of data wiping in safeguarding national security. Senior staff officers at the RMAF headquarters, Ministry of Defence (MINDEF), are given laptops for work-related purposes. As such, the laptops might contain secret and top-secret work-related documents. When the officer is posted out from MINDEF, laptops will have to be returned. Malaysia is experiencing rapid economic growth and digital transformation, but it faces cybersecurity challenges that threaten its stability. Cyber threats come from various sources, leading to data breaches and other incidents. Data wiping, the secure erasure of data from storage devices, is crucial for protecting sensitive information. The Personal Data Protection Act (PDPA) requires organizations to implement data erasure measures. This paper aims to explore the current data wiping practices in the RMAF.

Keywords: Data Wiping · Secret · Military · Cybers threats

1 Introduction

Cyber threats in Malaysia come from various sources, including hackers, cybercriminals, state-sponsored actors, and insiders. These threats can lead to data breaches, identity theft, financial fraud, espionage, and other cyber incidents that can have severe consequences for individuals, organizations, and the nation as a whole [1].

Data wiping is a critical security measure that can help to protect the data of the Malaysian Armed Forces (MAF) from cyber-attacks. Data wiping, also known as data sanitization, is a technique used to securely erase data from storage devices to ensure that it cannot be accessed or recovered by unauthorized individuals. The primary goal of data wiping is to overwrite the existing data with random or predefined patterns, making it irretrievable using standard data recovery methods [2].

The Personal Data Protection Act (PDPA) is one of the main data protection laws in Malaysia that governs the collection, processing, and handling of personal data. The PDPA requires organizations to implement appropriate measures to protect personal data, including ensuring that data is securely erased when it is no longer needed. Failure

H. Badioze Zaman et al. (Eds.): IVIC 2023, LNCS 14322, pp. 328–338, 2024.
https://doi.org/10.1007/978-981-99-7339-2_28

to comply with the PDPA can result in legal and financial consequences, including fines and imprisonment [3].

The MAF is also aware of how crucial data erasure is to maintaining national security. The MAF has implemented various policies and procedures for data wiping, including the use of advanced data wiping technologies and periodic audits of data wiping practices. However, despite the legal and institutional framework for data wiping in Malaysia, there are still challenges and gaps. Many organizations, including government agencies, private entities, and individuals, lack awareness, knowledge, and skills related to data wiping, resulting in inadequate or ineffective data wiping practices.

Therefore, there is a need for research on data wiping practices in Malaysia to identify gaps, challenges, and best practices, and propose recommendations to improve the effectiveness and compliance of data wiping practices. Such research can help mitigate cybersecurity risks, protect national security, comply with data protection regulations, maintain organizational reputation and trust, and advance knowledge and best practices in the field of cybersecurity.

In the Defence White Paper 2020, the Ministry of Defence emphasizes the need for a holistic approach to cybersecurity that encompasses various areas such as personnel, processes, and technology [4]. This includes adequately training personnel in cybersecurity best practices, as well as the development of robust policies and procedures for data protection, including the secure wiping of data. Proper data wiping is critical to preventing sensitive information from falling into the wrong hands, whether through malicious intent or accidental data breaches [5]. This is particularly important in the defence sector, where the loss of sensitive information could compromise national security and put lives at risk [6].

These measures include the use of specialized software and tools for data wiping, as well as the implementation of policies and procedures for the secure storage and disposal of sensitive information. The Ministry of Defence also conducts regular audits and assessments of its cybersecurity measures to ensure that they remain effective and up-to-date. In addition to these measures, the Ministry of Defence also emphasizes the need for ongoing cybersecurity education and training for all personnel, from senior leadership to frontline employees. This includes not only technical training on cybersecurity tools and procedures but also developing a culture of cybersecurity awareness and vigilance. Cybersecurity Malaysia is a government agency entrusted with the responsibility of protecting Malaysia's cyberspace and ensuring the safety and security of its digital infrastructure [7].

In August 2020, a report revealed that 70 sensitive Royal Malaysian Navy (RMN) documents were sold on the dark web, posing a significant risk to national security. The documents, which contained classified information such as ship logs and technical specifications of the naval vessels, were reportedly stolen by hackers or insiders who gained unauthorized access to RMN's computer systems [8].

The incident highlights the importance of effective cybersecurity measures, including data wiping, to prevent data breaches and cyber threats in the MAF. Data wiping is the secure deletion of data from storage devices to prevent unauthorized access and data recovery. In the case of the RMN, it is unclear if the data on the compromised systems was wiped, which could have potentially prevented the stolen data from being sold on the dark web [8].

This research aims to improve RMAF cybersecurity by ensuring that sensitive and confidential data is properly erased from storage devices, rendering it inaccessible to unauthorized individuals or entities. Enhancing data wiping practices can significantly reduce the risk of data breaches, identity theft, data leaks, and other cybersecurity incidents, which can have severe consequences for individuals, organizations, and the nation as a whole. To achieve this goal, the research will employ an appropriate approach to assess the awareness, knowledge, and practices of data wiping within the RMAF.

The rest of this paper is organized into several sections. Section 2 explores the concept of data wiping and prevalent techniques, as well as how the military handles data. Section 3 discusses the importance of Data Wiping in Cybersecurity. Section 4 discusses the current data wiping practices of the Royal Malaysian Air Force (RMAF). Finally, we conclude this paper with future work in Sect. 5.

2 Background and Related Work

In this section, some background information on data wiping practices is discussed.

2.1 Data Wiping

Data wiping is considered as one of the anti-forensic techniques. On the other hand, data sanitization, also known as data wiping, is a method used to ensure that unauthorised individuals do not have access to the deleted data [2]. This process overwrites the existing data with random or meaningless information, making it unrecoverable even with advanced forensic techniques [9]. This is crucial to prevent unauthorized access to sensitive information and to ensure data privacy and security [10]. Proper deletion of data wiping is crucial for compliance with data protection regulations. There are two main approaches of data wiping: (i) partition wiping and (ii) file wiping.

- Partition Wiping: This approach focuses on wiping an entire partition on a storage device. It involves the following aspects:

  a. NTFS Volume Boot Record (VBR): The first case of partition wiping relates to the VBR, which is a structure in the header of the NTFS file system. Some partition wiping tools create the VBR structure after the wiping process. If the wiping tool does not generate the VBR, the partition is considered unusable and requires formatting to be used again.
  b. Overwritten Data Type: The second case of partition wiping is related to the type of data overwritten during the process. Different data sanitization standards may be implemented in various ways. Some methods use a random pattern, while others utilize a random specific hex value. The choice of approach can affect the entropy values of the overwritten data. Random patterns yield higher entropy values closer to one, whereas a focus on specific random values yields entropy values closer to zero.

- File wiping is considered one of the basic and fundamental techniques for preserving privacy and ensuring data security. It involves overwriting the data within individual files to make them unrecoverable [11]. It includes the following considerations:

  a. File Types: File wiping encompasses three types of files. The first type is the file itself, which contains both file system metadata and actual data. These files can be checked by both the Windows Operating System and file wiping tools.
  b. Deleted File Metadata: The second type consists of files that appear as deleted in the Master File Table (MFT) entry but still retain recoverable data. Although these files are not visible in the Windows OS, file wiping tools or digital forensic tools can identify them. By applying data sanitization standards, the actual data of these files can be changed to a non-recoverable state.
  c. Deleted File Metadata: The second type consists of files that appear as deleted in the Master File Table (MFT) entry but still retain recoverable data. Although these files are not visible in the Windows OS, file wiping tools or digital forensic tools can identify them. By applying data sanitization standards, the actual data of these files can be changed to a non-recoverable state.
  d. Overwritten Metadata and Data: The last type includes areas where both the metadata and actual data of a file are overwritten, including slack areas. Even in these areas, fragments of data may be recoverable. However, a file wiping tool can use data sanitization standards to overwrite the remaining data in the slack area, making it non-recoverable [12].

There are several methods available to ensure the secure disposal of information. Three common methods are discussed in this section: Clear, Purge and Destroy [19]. To determine the appropriate method, users should consider the type of information, the storage medium, the risk to confidentiality, and future plans for the media. Factors such as cost and environmental impact should also be considered when assessing the selected method. The goal is to choose a sanitization method that effectively mitigates the risk of unauthorized disclosure of information [13]. NIST provides guidelines and standards for secure data destruction, including recommendations for the clear/purge process on different types of media, such as flash memory. Media sanitization consists of three processes: clear, purge and destroy.

- Clear. This process involves replacing the target data with non-sensitive information, including both the logical storage location of files and all user-accessible areas. However, it is important to note that overwriting may not be suitable for damaged or non-rewriteable media, and it may not address all areas where sensitive data can be retained. Factors such as media type, size, and technology (such as flash memory-based devices with wear leveling) can affect the feasibility of overwriting. In cases where dedicated storage devices are not involved, such as basic cell phones or office equipment, the "Clear" operation may refer to returning the device to its factory state or deleting file pointers, as these devices may not support direct rewriting or media-specific techniques. In such cases, manufacturer resets or procedures that do not involve rewriting may be the only option for clearing the device and associated media, as long as the user interface does not allow retrieval of the cleared data [13].

- Purge. The process of purging data from media involves various methods that must be applied with consideration for the specific media type. These methods include overwrite, block erase, and cryptographic erase, using dedicated device sanitize commands that employ media-specific techniques. Destructive techniques such as incineration, shredding, disintegrating, degaussing, and pulverizing can also effectively purge the data by rendering the media unusable and making data recovery infeasible. However, certain methods like bending, cutting, and some emergency procedures may only damage the media partially, allowing for potential data recovery through advanced laboratory techniques. Degaussing, when properly matched to the media's coercivity, can purge legacy magnetic devices, but it should not be solely relied upon for flash memory-based or magnetic devices containing non-volatile non-magnetic storage. It is important to consult the device manufacturer for coercivity details. Degaussing may render many types of devices unusable, effectively acting as a destruction technique as well [13].
- Destroy. Media destruction is an important aspect of data sanitization, and various techniques and procedures are available for this purpose. Complete destruction of media can be achieved through methods like disintegration, pulverization, melting, and incineration. These methods are usually carried out by specialized facilities with the necessary capabilities. Shredding is another effective technique, particularly for flexible media like diskettes, where the media is physically removed from its container and shredded into small pieces to prevent data reconstruction. To further enhance security, the shredded material can be mixed with non-sensitive material of the same type. Destructive techniques become necessary when other clear or purge methods are not applicable or fail to effectively sanitize the media. These techniques ensure that the target data becomes infeasible to retrieve both through device interfaces and state-of-the-art laboratory techniques, providing a robust level of data protection [13].

2.2 Common Technique Used in Data Wiping

Scholars [14, 15] have listed several data wiping techniques/standards are most commonly used in various data wiping methods. The DoD 5220.22-M method offers two main variants: 3-phase and 7-phase. This method is developed and supported by the US National Industrial Security Program. The algorithm consists of several steps: writing zeros and verifying; writing ones and verifying; and writing random characters and verifying. By following this sequence, the method is intended to ensure the effective erasure of data from the storage device.

The NCSC-TG-025 method is a standard developed and supported by the US National Security Agency (NSA). It builds on the DoD 5220.22-M wiping techniques but provides additional options, particularly with respect to the number of overwriting processes. This standard offers more flexibility in selecting the number of overwrites performed during the data wiping process. It is developed to improve security and data erasure capabilities, aligning with the requirements of national security organizations.

The AFSSI-5020 method is a standard developed and supported by the United States Air Force. It is similar to the DoD 5220.22-M method, but it differs in the verification process during the last step. The AFSSI-5020 process involves writing 0 to the storage device, followed by writing 1, and then a random character. However, the specific difference lies in the verification step during the final phase. This method is designed to meet the data wiping requirements of the United States Air Force, ensuring secure and reliable erasure of sensitive information.

The AR 380-19 method is a standard developed and supported by the United States Army. It has a distinct process for data wiping, consisting of several phases. In this method, the process involves writing a random character to the storage device, followed by writing a typical character. Next, a specified character complement is written, and the verification of the written data is performed. This standard is designed specifically to meet the data wiping requirements of the US Army, ensuring the secure and effective erasure of sensitive information from storage devices.

The NAVSO P-5239-26 method is a standard developed and supported by the United States Navy. It provides guidelines for secure data wiping from storage devices. The process involves several steps, including writing a specified character to the storage device, followed by writing the typical character complement. Then, a random character is written, and the verification process is performed to ensure the integrity of the data wiping. This method is specifically designed to meet the data sanitization requirements of the US Navy, ensuring the proper removal of sensitive information from storage devices.

The Gutmann 35-passes method, developed by Peter Gutmann, was once considered a highly secure data wiping method. This method involves performing 35 passes, during which a random character is repeatedly written to the storage device. While this method was designed with the intention of ensuring data erasure, its effectiveness on modern storage devices is questionable. Newer data wiping methods, such as those mentioned earlier, have been developed to address the challenges and complexities associated with modern storage technologies.

The Schneier method, developed and supported by Bruce Schneier, is a data wiping technique that involves 7 passes to securely erase information from a storage device. The process includes the following steps: (i) Writing 1 to the storage device, (ii) Writing 0 to the storage device, and (iii) Writing a pattern of random characters in the next 5 passes. By performing these 7 passes, the Schneier method aims to make it difficult for any data recovery attempts, enhancing the security of data erasure on the storage device.

2.3 Data Handling in Military

According to the Malaysian Armed Forces Staff Manual (Service Writing) [16], the security classification system used by the MAF is standard across the various services under the MAF. The security classification is assigned to documents based on the level of security information they contain and indicates the potential risk to national or international security if the information is disclosed without authorization. The purpose of the security classification is to ensure appropriate protection and control of sensitive information. The security classifications used within the MAF are as follows:

- TOP SECRET (RAHSIA BESAR). Information and material, the unauthorized disclosure of which would cause exceptionally grave damage to the nation. This could include information about the location of weapons, the identity of undercover agents, or the details of a pending military operation.
- SECRET (RAHSIA). Information and material, the unauthorized disclosure of which would damage the interests of the nation. This could include information about troop movements, weapons systems, or intelligence gathering.

- CONFIDENTIAL (SULIT). Information and material, the unauthorized disclosure of which would be prejudicial to the nation's interests. This could include information about personnel records, financial information, or operational plans.
- RESTRICTED (TERHAD). Information and material, the unauthorized disclosure of which would be undesirable to the interests of the nation. This could include general information about the military, training materials, or administrative procedures.

The primary objective of this manual is to offer comprehensive guidelines for the effective management of security within the MAF. A key aspect of security management involves understanding and leveraging military intelligence derived from various textual sources. These sources include smartphone texts, email communications, social media posts, and documents. RMAF personnel are therefore required to exercise careful analysis and comprehension of the data and information shared through these textual sources. The ease of data sharing facilitated by modern devices emphasizes the importance of a thorough understanding of the content being shared. By ensuring a meticulous grasp of this information, RMAF personnel can enhance their ability to extract valuable intelligence while upholding security measures within the organization.

Proper device disposal is paramount for organizations to mitigate risks and uphold data confidentiality. Inadequate disposal practices can result in legal and ethical implications due to potential data confidentiality breaches. To address this, implementing a policy that outlines appropriate procedures for cleaning or destroying devices containing sensitive and confidential data, as well as licensed software, is crucial [17]. Mitigating these risks requires robust security measures, employee training, and proper data management protocols.

3 The Importance of Data Wiping in Cybersecurity

3.1 Data Wiping Guidelines in the Military

The guidelines or manuals within the MAF serve as documented references for each headquarters and unit. These documents outline the policies and guidelines specifically related to cybersecurity in the MAF. Some of the key policies and guidelines that pertain to cybersecurity within the MAF are as follows:

- *Defence White Paper*. This paper is a strategic document that outlines the requirements, goals, and priorities for the defence sector of a country. It serves as a guiding document for the military and defence organizations in safeguarding the nation's interests, sovereignty, and security. In the context mentioned, the Defence White Paper highlights the need for the MAF to address emerging challenges, including cyber warfare, in order to protect the country's interests in the modern warfare environment.
- *Polisi Keselamatan Siber MAMPU*. This policy is a comprehensive policy framework utilized by government agencies to effectively manage cybersecurity and information and communication technology (ICT) within their organizations. This policy aims to provide guidelines and best practices for ensuring the confidentiality, integrity, and availability of digital assets, as well as protecting against cyber threats and risks.

- *Information and Communication Technology Security Policy v5.0.* This policy sets out the framework and requirements for ensuring the security of information and communication technology systems within MINDEF. It applies to all civilian and armed forces personnel who have access to or are responsible for MINDEF's ICT infrastructure and resources.
- *General Order of the Armed Forces (PAAT 1/13).* This directive serves as a comprehensive guideline for all armed forces personnel regarding the usage of the internet and intranet. The directive outlines specific prohibitions and restrictions in order to ensure the secure and appropriate use of these communication platforms within the armed forces.
- *General Order of the Armed Forces 3/13 (PAAT 3/13).* This directive specifically addresses the usage of social media platforms by armed forces personnel. This directive serves as a comprehensive guideline to ensure responsible and appropriate behaviour in the online social media environment, while upholding the reputation and integrity of the armed forces.
- *Malaysian Armed Forces Security Order 2019.* This recent publication consolidates various Acts and orders within the MAF. Serving as a comprehensive guide, this security order is intended to be followed by all MAF leadership and personnel. It is essential for every individual within the MAF to have a thorough understanding of this document. By encompassing relevant legislation and directives, the Malaysian Armed Forces Security Order 2019 provides a unified framework to ensure adherence to security protocols and procedures throughout the organization.
- *Manual Pengurusan ICT Bahagian Komunikasi Dan Elektronik 2021.* This manual provides guidance and procedures for managing information and communication technology (ICT) in the Communication and Electronics Division. The manual covers various aspects, including ICT infrastructure management, network administration, data management, and security protocols. It serves as a reference for personnel involved in ICT operations, emphasizing the importance of efficient and secure ICT practices to ensure smooth operations within the division. The manual aims to establish standardized procedures and guidelines for the effective management of ICT resources and to promote a secure and reliable ICT environment within the division.

3.2 Data Sanitization in Organization

NIST had different procedures and guidelines. The guidelines mentioned in this section emphasize the importance of media reuse within the Department of Defence (DoD) while ensuring the complete removal of data and information from operable media. Here is a more detailed summary:

- *Media Reuse.* The objective is to sanitize media to ensure that no data or information remains on media that are to be reused within the DoD.
- *Clearing and purging.* For unclassified media, it is necessary to clear the data before reuse. This involves removing all data from the media, ensuring that no sensitive information remains. Media containing sensitive data, excluding Controlled Unclassified Information (CUI) or Personally Identifiable Information (PII), should be purged before reuse. Purging ensures that any residual data is thoroughly removed from the

media, rendering it unrecoverable. The National Institute of Standards and Technology Special Publication 800-88 provides detailed guidelines and references for implementing these sanitization practices.

- *Complete Data Removal.* To ensure the removal of data from information systems, storage devices, and peripheral devices with storage capacity, various methods can be employed. These methods include degaussing (erasing magnetic fields), smelting, incinerating, disintegrating, or pulverizing the media. The goal is to render the stored information completely unrecoverable, preventing any potential reconstruction.
- *Classified Media Reuse.* For classified media, it is essential to clear the data before reuse and limit the reuse to classified environments. Chairman of the Joint Chiefs of Staff Instruction 6510.01F provides specific instructions and guidelines for clearing and reusing classified media. It is crucial to ensure that classified storage media is not sanitized and declassified for reuse in an unclassified environment to maintain the integrity and security of classified information.
- *Spillage Events.* In the case of spillage events, where classified or sensitive information may have been inadvertently disclosed or compromised, the current 624 Operations Centre Tasking Order should be consulted for appropriate procedures and actions to be taken.

4 Current Data Wiping Practices of the RMAF

The *Manual Pengurusan ICT Bahagian Komunikasi Dan Elektronik 2021* identifies two categories of risks associated with personal mobile devices: (a) device-related risks and (b) application-related risks [18]. Device-related risks stem from the storage of data internally or in the cloud, information transmission outside the organization, and device loss. The RMAF has less control over personal mobile devices compared to provided personal computers or laptops. Application-related risks arise from the downloading and installation of third-party mobile applications that interact with official organizational data stored on the devices. To address these risks, the manual suggests four steps for ensuring the security of personal mobile device usage:

- *Step 1: Risk Reduction through Mobile Device Management (MDM).* Organizations should identify and register authorized personal mobile devices accessing official data. Official information should be classified, and allowed devices and applications should be determined based on the classification. MDM tools can assist with device configuration, software and application distribution, encryption, password administration, remote wipe, and lock
- *Step 2: Risk Reduction in App Downloads through Guidelines and Awareness Campaigns.* Downloaded applications from unknown sources pose significant security threats. Establishing control over application downloads and promoting awareness among RMAF personnel can mitigate these risks. Trusted app stores should be used for application downloads.
- *Step 3: Internal Application Development.* Developing internal mobile applications with authentication mechanisms before accessing organizational data is recommended as the third step. This approach reduces reliance on downloading apps from untrusted sources.

- *Step 4: Conducting Security Audits on Devices, Infrastructure, and Mobile Applications*. Comprehensive security audits should be performed to assess mobile device infrastructure, conduct penetration tests on devices and servers, evaluate application security for potential information leaks, and assess the alignment of instructions and procedures with best practices.

However, the current practice of laptop policy in RMAF involves passing on laptops without performing any data wiping. This means that when laptops are transferred or reused within RMAF, the data stored on them is not properly erased or sanitized. This practice poses a significant risk in terms of data security and confidentiality.

5 Conclusion

In conclusion, data wiping is a critical aspect of cybersecurity to protect sensitive information from unauthorized access and data breaches. RMAF recognizes the importance of data wiping in safeguarding national security and has implemented various guidelines and policies to ensure secure data disposal. However, there are challenges that need to be addressed, including awareness and knowledge gaps among personnel, limited resources and infrastructure, compliance with regulations, integration with existing systems, and keeping up with evolving threats. By addressing these challenges and enhancing data wiping practices, the RMAF can strengthen its cybersecurity posture, mitigate risks, and ensure compliance with data protection regulations. This research aims to explore the current data wiping practices in the RMAF, propose guidelines for improvement, and verify the effectiveness and compliance of data wiping guidelines. By doing so, it will contribute to the overall enhancement of data security within the RMAF and the protection of sensitive information.

References

1. Malaysia Cyber Security Strategy 2020–2024. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf. Accessed 25 May 2023
2. Yusof, N.A.B., Abdullah, S.N.H.B.S., bin Md Senan, M.F.E., Sahri, M.B.: Data sanitization framework for computer hard disk drive: a case study in Malaysia. Int. J. Adv. Comput. Sci. Appl. **10**(11), 398–406 (2019)
3. Laws of Malaysia - Personal Data Protection Act 2010. https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf. Accessed 27 May 2023
4. Defence White Paper. https://www.mod.gov.my/images/mindef/article/kpp/DWP-3rd-Edition-02112020.pdf. Accessed 20 June 2023
5. Shivashankar, M., Mary, S.A.: Privacy preservation of data using modified rider optimization algorithm: optimal data sanitization and restoration model. Expert. Syst. **38**(3), e12663 (2021)
6. Mat, B., Pero, S.D.M., Wahid, R., Shuib, M.S.: Cyber security threats to Malaysia: a small state security discourse. Sustain. Glob. Strateg. Partnership Age Uncertainties **5**(6), 31 (2020)
7. CyberSecurity Malaysia. https://www.cybersecurity.my/data/content_files/46/880.pdf. Accessed 20 June 2023
8. Malaysian Navy RMN papers put up on Dark Web - MY Military Times, 29 July 2023. https://mymilitarytimes.com/index.php/2020/08/17/malaysian-navy-rmn-papers-put-up-on-dark-web/. Accessed 20 June 2023

9. Borham, N.A.M., Mohamad, K.M.: DocWIPE: data wiping tool using randomized 512-gram. Appl. Inf. Technol. Comput. Sci. **2**(2), 155–164 (2021)
10. Reardon, J., Basin, D., Capkun, S.: SoK: secure data deletion. In: Symposium on Security and Privacy, pp. 301–315 (2013)
11. Wani, M.A., AlZahrani, A., Bhat, W.A.: File system anti-forensics–types, techniques and tools. Comput. Fraud Secur. **2020**(3), 14–19 (2020)
12. Oh, D.B., Park, K.H., Kim, H.K.: De-Wipimization: detection of data wiping traces for investigating NTFS file system. Comput. Secur. **99**, 102034 (2020)
13. Kissel, R., Regenscheid, A., Scholl, M., Stine, K.: Guidelines for media sanitization, pp. 800–888. US Department of Commerce, National Institute of Standards and Technology (2014)
14. Wei, M., Grupp, L., Spada, F.E., Swanson, S.: Reliably erasing data from {flash-based} solid state drives. In: 9th USENIX Conference on File and Storage Technologies (FAST 11) (2011)
15. Ölvecký, M., Gabriška, D.: Wiping techniques and anti-forensics methods. In: 16th International Symposium on Intelligent Systems and Informatics (SISY), pp. 000127–000132 (2018)
16. E-Doktrin. https://www.airforce.mil.my/index.php/en/informasi/penerbitan/e-doktrin. Accessed 29 July 2023
17. Hughes-Lartey, K., Li, M., Botchey, F.E., Qin, Z.: Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon **7**(3) (2021)
18. Manual Pengurusan ICT Bahagian Komunikasi Dan Elektronik. In Portal Rasmi TUDM. https://www.airforce.mil.my/index.php/bm/allcategories-ms-my/informasi/penerbitan/manual-pengurusan-ict-bahagian-komunikasi-dan-elektronik. Accessed 29 July 2023
19. Ahn, N.Y., Lee, D.H.: Schemes for privacy data destruction in a NAND flash memory. IEEE Access **7**, 181305–181313 (2019)