Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

DATA SECURITY RISKS ON SOCIAL MEDIA FOR THE MILITARY

Leli Setyaningrum*[1], Saravia Luciano[2], Zainal Syahlan[3]

***[1,3]Information Technology Department, Naval Technology College (STTAL), East Java, Indonesia 60178**
[2]Training School, Military Institute of Weapons and Specialties, Montevideo, Uruguay 13000

***[1]Email: leli.setyaningrum@gmail.com**
[2]Email: lucesaravia@gmail.com

Abstract
Modern military organizations are influenced by the development of information technology that continues to innovate and the demands of speed and accuracy of data and information. The importance of data security in using social media for the military requires security methods with different specifications to protect the confidentiality of data, especially regarding military operations. The use of qualitative methods with a grounded theory approach provides an understanding of the phenomena that are occurring in the research object. The existence of social media to date, cannot be denied based on existing data, has a big influence on the environment and operations in the military, so there is a need for the development of data or social media security methods with special specifications for the military, both in the form of cryptography with the development of encryption algorithms and their descriptions, as well as innovations for special models of data and information security in the military environment.
Keywords: *social media; cyber security; military operations; military information*

INTRODUCTION

Social media is a form of technology development that can be used easily and has a function to connect people who are in different places, by utilizing the internet. In addition, social media is also a place for education, a source of various information, strengthening self-identity, associating with various organizations, and marketing commodities (Craig et al., 2017; Jenny, 2015; Major Cybercrime Unit (MCU), 2021; Yohanna, 2020). The development of communication technology that can provide complete facilities, and convenience, both in terms of format, function, and speed of delivery time, provides innovation and a different experience compared to previous communication technology. With the use of the internet which is very interactive various developments can be facilitated both in collaborative and individualistic forms, by accommodating facilities for creating, sharing content, and supporting social network sites (Jenny, 2015; Sangeeta Bhat, 2024).

In military organizations, there has also been a lot of use of social media, including sharing various information such as location, education, articles/news, reports, family, and others. This has become a common activity, even though it should be confidential or very confidential. There is also information about operations that should not be allowed to be distributed freely but can be read because of sharing via social media. So, it is necessary at an urgent level, for a very high level of protection for social media models that can be used in military

Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

organizations, with limited access to certain parties, equipped with monitoring and control in use and its protection (Major Cybercrime Unit (MCU), 2021).

Increased protection on the social media model used, not only protects the content and information processed in it but also the various functions in the application. The social media model for military organizations requires a level of protection that can protect against all forms of leaks, attacks, information infiltration, and threats arising both in the application and the data and information contained therein. The existence of social media also makes it easier for soldiers to communicate as users, with family and other parties, but the form of information shared can have a negative impact on the organization, especially if it contains information related to military service and operations (Major Cybercrime Unit (MCU), 2021; Yohanna, 2020).

By using Internet of Things (IoT) ecosystem technology in the use of social media, there are several weaknesses and challenges that must be overcome carefully, namely security and privacy of data and information. (Zhang & Wang, 2024). The proposed social media model for military organizations should also have cyber security technology to protect various forms of data and information in communication in social media, this is an effort to protect various forms of information regarding military operations and other information. Through the development of a military-specific social media model that has cryptographic techniques with encryption and description algorithms that can provide maximum protection for the social media path used.

Security methods for various data and information are crucial and have a big impact, both on personnel and organizations in the military environment. This is related to confidential data traffic and can sometimes appear on social media, especially related to military operations or other military information. Ultimately, the data security method is also related to cyber security, namely cryptography which uses encryption-description algorithms for data moving in social media. This algorithm must be able to protect data well and specifically for the needs of military data protection.

Several encryption and decryption algorithms have been developed, used, and included in cryptographic techniques. The encryption/decryption process is carried out using several keys, with the key in the description being a key that is difficult to solve, without the help of an encryption key. Figure 1 shows the cryptographic techniques that have existed until now, namely asymmetric keys, symmetric keys, and hashing (Alenezi et al., 2020).

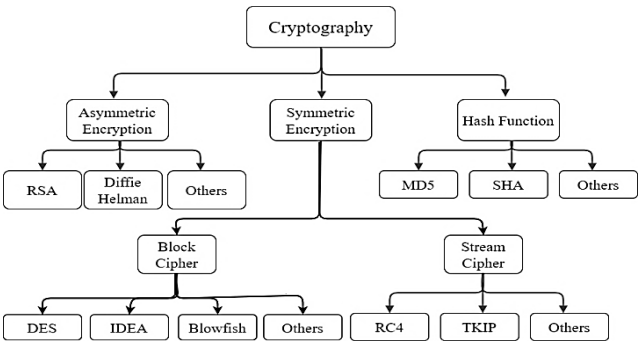

Figure 1. Cryptography technique

Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

In symmetric key techniques, the encryption and decryption process is based on one key, namely the private key, that sharing it with the recipient and sender requires a secure channel and has a type based on input data: stream cipher and block cipher. Cryptographic techniques for asymmetric keys use two keys, one secret key for the decryption process, and a public key for the encryption process. However, this technique is less appropriate for use on large documents because of the slow problem of the key-matching process and the relatively large level of CPU usage. Hashing is a mathematical algorithm that maps an input message in various sizes into a bit string with a fixed size or hash (Alenezi et al., 2020; Fitzpatrick, 2021; Tyagi & Ganpati, 2014).

MATERIALS AND METHODS

The use of grounded theory in qualitative research provides the ability for research to develop a form of theory based on existing data obtained through the literature review process and understanding of the military environment through environmental literacy activities, thus supporting the drawing of final conclusions and exploring the problems that occur (Ayu & Budiasih, 2013).

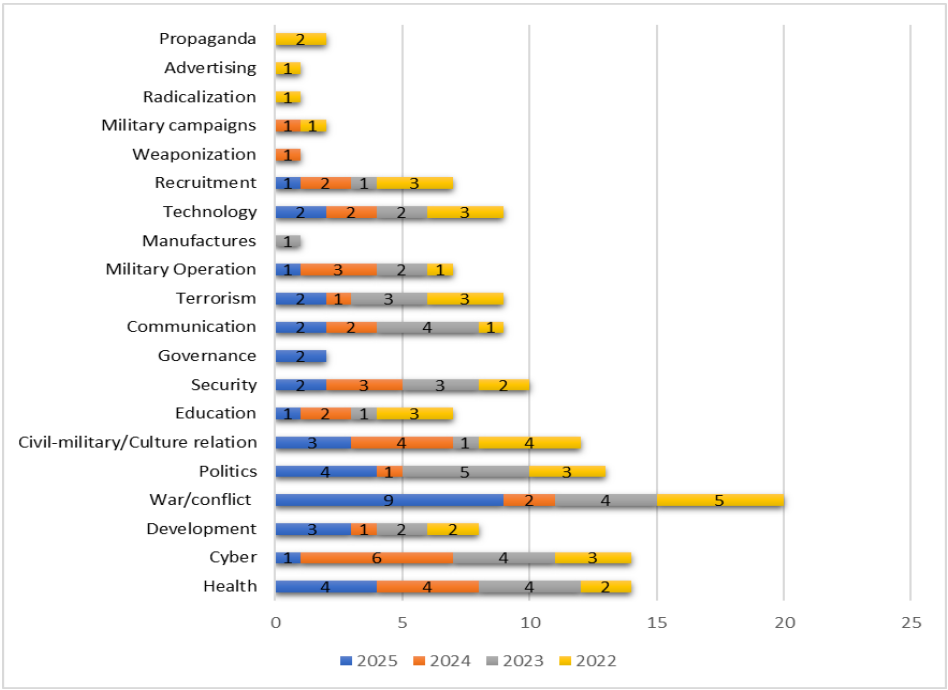

Figure 2. The use of social media in the military 2022 -2025

Research on the use of social media for the military has been conducted in previous studies, focusing on various fields – for example, as seen in Figure 2, so there must be an effort to develop security methods that can be applied to protect the data and information contained therein. In this study, samples were taken from various fields that have been discussed in previous studies, and there were 149 articles with a range of 2022-2025, related to social media used in the military environment, to obtain limitations on its use. However, based on environmental literacy that was carried out, through observations in the military service environment and assignments in several countries, the use of social media in the military is increasingly widespread and often unprotected by a security system for data and information. Secret military operations can be open to being known by

Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

other parties because there are forms of reports sent via social media. Likewise, military information, which does not have special protection, is sent via social media.

RESULTS AND DISCUSSIONS

Cryptography

Cryptographic technology is a security service used to ensure that there is protection for data and is not misused, by changing plain text to coded text (Pronika & Tyagi, 2021). The main goal is to achieve security for data and information that is closely related to authentication, confidentiality, access control, data and information integrity, and availability (Al-Shabi, 2019). There are three types of cryptographic techniques, namely:

a. *Symmetric Encryption*
   There are two types based on data input, namely block ciphers, which encrypt data in a group of bits called blocks with a fixed length, and stream ciphers, which process data on a stream of bits (Alenezi et al., 2020).
b. *Asymmetric Encryption*
   Known as a public key but uses a private key to decrypt messages that are only known to the recipient of the message (Asaithambi, 2015).
c. *Hashing*
   Hash functions to store passwords and check data integrity (Alenezi et al., 2020).

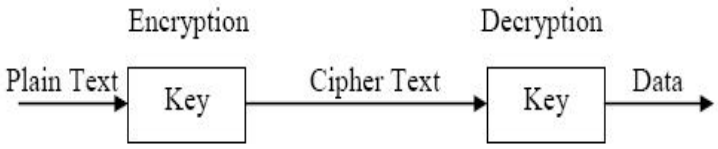

Figure 3. Alur Kriptografi (Kaushik et al., 2023)

Realizing the increasing use of electronic data which also increases security risks, various encryption algorithms have been developed that are already standard and available to the public (DeCannière et al., 2006). With the increasingly massive use of encryption algorithms, it can also be developed on social media with a special encryption model for the military environment, which can provide better security for military data and information flows in it so that the military has its own social media platform that is only used in the military environment.

The use of Social Media in the Military

The development of communication technology that influences changes in the communication style itself, shows that there is an increase in the social lifestyle of humans.

Table 1. The development and use of social media in military and cyber security (example discussion based on previous research)

Num.	References	Sample Objects	Subjects	Security considerations
Utilization and development of social media in the military				
1	(Coronges et al., 2012)	Army at all ranks	social media	the security risks
2	(Sarah &	British military	Social media	lack of security

Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

	Helen, 2016)			
3	(Herrick, 2016)	Russia-Ukraine ISIS	The operations of military social media and cyber operations	security discussed
4	(Craig et al., 2017)	Swiss Armed Forces	Social media	security discussed
5	(Veerasamy & Labuschagne, 2018)	south africa	Social media	security discussed
6	(Mangat, 2018)	Canadian Armed Forces	Twitter	security focus on content
7	(Jodel, 2020)	military community	social media platforms provide service members	lack of security
8	(Peralta & Caporusso, 2020)	Delayed Entry Program (DEP)	Social Networks (e.g., Facebook, Instagram, and LinkedIn) as a recruiting tool	lack of security
9	(Grigorescu, 2024)	US military personnel, British Army	military recruitment through social media	under consideration, regarding the risks
10	(Rahman & Shurong, 2024)	Pakistani military's	The influence of military-linked Social Media Activists (SMA) on the implementation of elections	security discussed
11	(Hasibuan & Lazuardi, 2024)	the Islamic teaching (Tabayyun)	Capabilities of integrating social media, toral politics	security discussed
12	(Radzi et al., 2025)	Military organizations	Conducting an evaluation of the use of social media in implementing military campaigns	under consideration, regarding the risks
Utilization of cyber security				
13	(Riadi et al., 2021)	Nasyiatul 'Aisyiyah and Muhammadiyah	social media services	cyber security

Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

		Youth		
14	(Sarjito, 2024a)	modern governments	The impact of cyber attacks on the effectiveness of data protection regulations and cybersecurity measures, public trust and government operations, and balancing transparency with prioritizing data security within the scope of open data initiatives.	security discussed
15	(Sarjito, 2024b)	national security	The influence of strategy, technological advances and geopolitical shifts as an effort to overcome various types of non-traditional security threats.	security discussed
Developments in social media utilization				
16	(Jenny, 2015)	social media technologies	Social media that has integration in an identity, interpersonal relationship institutions, economy and politics.	lack of security
17	(Shallcross, 2017)	United States Army	Benefits of cyber space from both internal and external aspects.	security discussed
18	(Yohanna, 2020)	Fourteen students of the Faculty of Social and Political Sciences, Universitas	Social media with positive and negative impacts of users on social interactions	lack of security

Nusantara Hasana Journal
Volume 4 No. 11 (April 2025), Page: 33-42
E-ISSN : 2798-1428

		Airlangga		
19	(Major Cybercrime Unit (MCU), 2021)	US Army Criminal Investigation Division (USACID)	Strengthening social media networks	the security and privacy settings for Facebook, Instagram, Twitter, and LinkedIn
20	(Sangeeta Bhat, 2024)	social media technologies	Social media's impact on business society, and especially teenagers	security discussed

Table 1 shows an example based on the discussion of previous research, by showing the use of social media in the military environment, cyber security related to the use of social media, and the development of social media itself. Some discussions pay close attention to data security issues, but some are general and do not pay attention to the security of the data and information in them. Along with the advancement of technology that continues to run without stopping, increasingly rapid and affects human life. The level of data and information security must also be a very important concern, especially for crucial aspects such as military data and information.

Communication technology that involves various technology platforms, such as the internet, causes the formation of unlimited communication by utilizing web platforms that can be accessed easily and quickly in all areas that have internet networks, both public and private, as well as various interesting content so that interactions are formed that go beyond the meaning of communication itself because of the functions, features, and innovations that continue to develop (Sangeeta Bhat, 2024).

The use of social media has also penetrated the military environment, various military-related information has been updated and shared openly, although there are several efforts such as cryptographic techniques for securing data sending and receiving. Several studies focus on social media in the military environment, each providing a different discussion according to the object and its use.

CONCLUSIONS & RECOMMENDATIONS

Social media has a very important position in life today, supported by technology that can provide the ability for humans to communicate far beyond the limits of distance and time. Technology with communication capabilities can provide many features that satisfy its users, ranging from text, images, and videos to various supporting features that complement the convenience of sharing information can be done. However, for the military, the use of social media should have its limitations and specifications supported by the protection of data and information more than social media platforms in general. There must be a social media model specifically intended for the military environment and can be accessed anywhere. This model must be equipped with a different encryption algorithm, with a high level of difficulty, but not difficult in the encryption-

description process it, become does not take a long time to translate various messages sent or received. Freedom in sending military data and information is needed, especially in the implementation of military operations, such as sending operational situation reports. In addition, this can also support communication with family, without worrying about information leaks, such as the position of personnel at a certain time.

REFERENCES

[1] Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. International Journal of Scientific and Research Publications (IJSRP), 9(3), p8779. https://doi.org/10.29322/ijsrp.9.03.2019.p8779

[2] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric Encryption Algorithms: Review and Evaluation Study. International Journal of Communication Networks and Information Security, 12(2), 256–272.

[3] Asaithambi, N. (2015). A Study on Asymmetric Key Cryptography Algorithms. International Journal of Computer Science and Mobile Applications, 3(4), 8–13.

[4] Ayu, I. G., & Budiasih, N. (2013). Metode Grounded Theory Dalam Riset Kualitatif. Jurnal Ilmiah Akuntansi Dan Bisnis, 9(1), 19–27.

[5] Coronges, K., E, S., & Chris, A. (2012). Generation 2.0: Social Media and the Future of the Army. Phalanx, 45(September), 27–29.

[6] Craig, D., Ketterer, S., & Yousuf, M. (2017). To Post or Not to Post. Journalism & Mass Communication Quarterly, 94(1), 168–188. https://doi.org/10.1177/1077699016684796

[7] DeCannière, C., Biryukov, A., & Preneel, B. (2006). An introduction to block cipher cryptanalysis. Proceedings of the IEEE, 94(2), 346–355. https://doi.org/10.1109/JPROC.2005.862300

[8] Fitzpatrick, P. (2021). Asymmetric Cryptography. Irish Mathematical Society Bulletin, 0020(January 1988), 21–31. https://doi.org/10.33232/bims.0020.21.31

[9] Grigorescu, I.-A. (Anca). (2024). Digital deployment: how social media can reshape modern military recruitment. European Student Think Tank. https://esthinktank.com/2024/07/30/digital-deployment-how-social-media-can-reshape-modern-military-recruitment/

[10] Hasibuan, F. D., & Lazuardi, A. (2024). Social Media Capabilities and Military Affairs Using Propaganda and Tabayyun in The Digital Warfare. Emerald: Journal of Economics and Social Sciences, 3(2), 65–78.

[11] Herrick, D. (2016). The social side of "cyber power"? Social media and cyber operations. International Conference on Cyber Conflict, CYCON, 2016-Augus, 99–111. https://doi.org/10.1109/CYCON.2016.7529429

[12] Jenny, L. D. (2015). Social Media. In G. Mazzoleni (Ed.), The International Encyclopedia of Political Communication, First Edition (Vol. 58, Issue 10, pp. 415–417). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118541555.wbiepc004

[13] Jodel. (2020). Military social media trends. BeckerDigital; BeckerDigital. https://www.becker-digital.com/blog/military-social-media-trends

[14] Kaushik, B., Malik, V., & Saroha, V. (2023). A Review Paper on Data

Encryption and Decryption. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(IV), 1986–1992.
[15] Major Cybercrime Unit (MCU). (2021). Social Media Protection : A Handbook For Security and Privacy Settings (Major Cybercrime Unit (MCU) Digital Persona Protection Program (DP3) (ed.); 2021st ed.). US Army Criminal Investigation Division (USACID).
[16] Mangat, R. (2018). Tweeting Strategy: Military Social Media Use as Strategic Communication [Wilfrid Laurier University]. https://scholars.wlu.ca/etd/2071
[17] Peralta, A., & Caporusso, N. (2020). The Impact of Social Media in Military Recruiting. Advances in Intelligent Systems and Computing, 1215 AISC(March), 415–420. https://doi.org/10.1007/978-3-030-51549-2_55
[18] Pronika, & Tyagi, S. S. (2021). Performance analysis of encryption and decryption algorithm. Indonesian Journal of Electrical Engineering and Computer Science, 23(2), 1030–1038. https://doi.org/10.11591/ijeecs.v23.i2.pp1030-1038
[19] Radzi, E. M., Abdullah, Khairul H.;Hazim, M., & Ghalib, A. (2025). Analyzing Social Media Approaches in Military Campaigns : a Scientometric and Scoping. 02(03), 109–122. https://doi.org/10.61552/SJSS.2025.03.001
[20] Rahman, S. U., & Shurong, Z. (2024). Military Organization's Use of Social Media and Its Relationship with Politics: Evidence from Pakistan. SAGE Open, 14(3), 1–15. https://doi.org/10.1177/21582440241264615
[21] Riadi, I., Khakim, M., & Rosyda, M. (2021). Pengembangan Cyber Security pada Layanan Media Sosial. Prosiding Seminar Nasional Hasil Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan, 944–950. http://www.seminar.uad.ac.id/index.php/senimas/article/view/7659
[22] Sangeeta Bhat. (2024). Impact of Social Media on Society. International Research Journal on Advanced Engineering Hub (IRJAEH), 2(03), 473–480. https://doi.org/10.47392/irjaeh.2024.0068
[23] Sarah, M., & Helen, T. (2016). The Digital Mundane, Social Media and The Military. Media, Culture and Society, 38(8), 1153–1168. https://eprints.whiterose.ac.uk/96172/3/the digital mundane. Media%2C Culture %26 Society. HT SM.pdf
[24] Sarjito, A. (2024a). Data Security and Privacy in the Digital Era : Challenges for Modern Government. JIAN (Jurnal Ilmiah Administrasi Negara), 8(3), 1–13.
[25] Sarjito, A. (2024b). Enhancing National Security: Strategic Policy Development in Defense Management. Jurnal Pelita Nusantara, 2(1), 56–68. https://doi.org/10.59996/jurnalpelitanusantara.v2i1.524
[26] Shallcross, N. (2017). Social Media and Information Operations in the 21st Century. Information Warfare, 16(1), 1–12. https://doi.org/10.1002/9781118381533
[27] Tyagi, N., & Ganpati, A. (2014). Comparative Analysis of Symmetric Key Encryption Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 4(8), 2277. www.ijarcsse.com
[28] Veerasamy, N., & Labuschagne, W. A. (2018). Framework for Military Applications of Social Media. International Journal of Cyber Warfare and Terrorism, 8(2), 47–56.

https://researchspace.csir.co.za/server/api/core/bitstreams/390008e7-c1da-4cf1-84bf-13172196b415/content

[29] Yohanna, A. (2020). The influence of social media on social interactions among students. Journal of Information and Knowledge Management, 12(02), 34–48. https://doi.org/10.1142/S0219649220500239

[30] Zhang, L., & Wang, L. (2024). A hybrid encryption approach for efficient and secure data transmission in IoT devices. Journal of Engineering and Applied Science, 71(1), 1–18. https://doi.org/10.1186/s44147-024-00459-x