UJoST
e-ISSN: 2962-9179
Universal Journal of Science and Technology

Vol. 4 No. 1(2025)

DATA SECURITY OF MEDICAL CHECKUP INFORMATION SYSTEM IN MILITARY HOSPITAL

Leli Setyaningrum[1], Zainal Syahlan[2], Isnadi[3]
[1,2,3] Information Technology Department, Naval Technology College (STTAL), East Java, Indonesia,
leli.setyaningrum@gmail.com , zsyahlan@gmail.com , isnadi071109@gmail.com

Abstrak

The medical checkup (MCU) information system is essential for maintaining activities in hospitals and health facilities. Development of a system that prioritizes the security of patient data and information contained therein. In military hospitals, patient condition data is soldier condition data that must be guaranteed security against various forms of data and information leaks. Thus, an appropriate security method is needed that can support the prevention of various forms of cybercrime attacks and data leaks. The military has more than one hospital that was established to support various military operations, so the system used is also an integrated system that can reach all existing hospitals and health facilities.

Kata kunci: medical checkup, cyber security, security data.

INTRODUCTION

Various innovations in the world of health continue to develop, including in information technology continues to change along with technological advances and needs, so that improvements in technological sophistication are part of solving problems for each case. Fundamental research activities related to health, public health, and others encourage the sustainability of the medical checkup (MCU) information system which is always up to date. However, along with technological developments, cyber crimes have also emerged which affect the data security of the system.

Technological developments are increasingly sophisticated with the continued digitalization technology that has reached many digital activities and transactions and is carried out online. This also has a negative impact with the increasing rampant cybercrime. The more sophisticated the technology, the more sophisticated the forms of crime such as phishing, hacking, and other negative activities. As the world becomes more digital, with more transactions and activities carried out online, the risk and impact of cybercrime are also increasing. Various reports, statistics, and expert analyses show the increasing frequency and sophistication of cybercrime, including hacking, phishing, ransomware, and other malicious activities (Kuzior et al., 2024). There are several types of individuals who are always involved in the world of the cyber attack industry, including “hacktivists,” criminals, spies, terrorists, and ethical hackers, who differ mainly based on their goals, legitimacy, and level of credentials..

A hospital is a place where someone undergoes treatment if they have health issues, by providing several alternative methods of health care services such as inpatient, outpatient, or health checks. MCU is an activity that should be carried out routinely and continuously, with examinations through clinical preventive services, so that a person's health condition can be known in depth (Grandis G. D. et al., 2022). For military personnel, MCU is a mandatory activity that must be carried out routinely or as needed and is one of the important requirements. However, the examinations carried out on military personnel have several differences, especially the health assessment standards and the stages of the procedure that are carried out more comprehensively. (Pardamean et al., 2012).

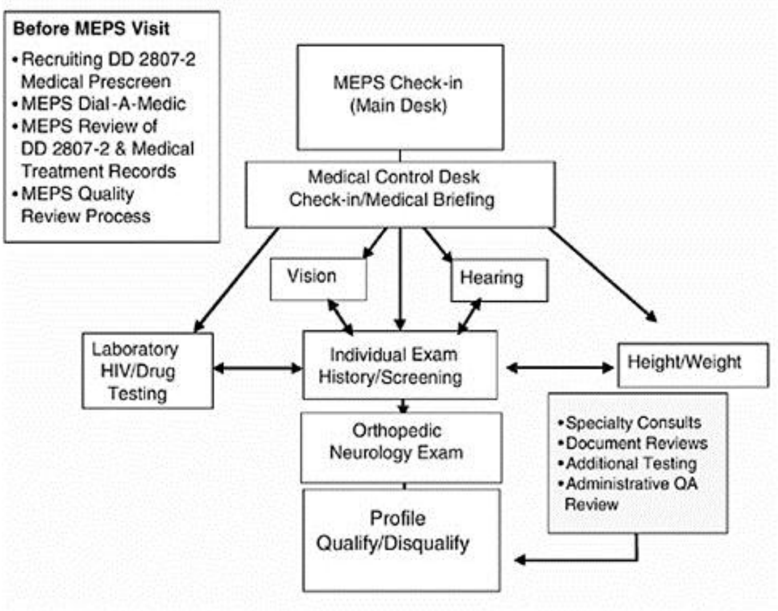
METHODS

The study uses the systematic literature review methods, by collecting journals, books, scientific papers, and articles on MCU, cybercrime, and other related subjects, which also have a relationship with the military field. In addition, continuous observation is also carried out, to produce final research results based on real conditions and previous research (Andriani, 2022). This is done to get results that can truly reflect the actual conditions so that the right solution can be found for the problems or gaps that arise. In addition, there are also several activities carried out, namely reviewing, identifying, evaluating, and interpreting other research with the same topic to obtain interesting phenomena (Crisnaldy, 2021).

RESULTS AND DISCUSSION

a. MCU military hospital

MCU is carried out routinely and continuously by military personnel to maintain the best health conditions so that it supports various operational tasks that must be carried out. Through several stages and procedures, MCU is carried out in stages for all types of examinations. There are several different types of examinations for certain personnel qualifications, for example, the special forces division which has a higher level of health assessment than other personnel. (Pardamean et al., 2012). Through Figure 1, we can see the stages of medical evaluation in the recruitment of military personnel when carrying out the MCU process, which is also carried out by military personnel as a whole.


Before MEPS Visit
•Recruiting DD 2807-2 Medical Prescreen
•MEPS Dial-A-Medic
•MEPS Review of DD 2807-2 & Medical Treatment Records
•MEPS Quality Review Process
MEPS Check-in (Main Desk)
Medical Control Desk Check-in/Medical Briefing
Vision
Hearing
Laboratory HIV/Drug Testing
Individual Exam History/Screening
Height/Weight
Orthopedic Neurology Exam
•Specialty Consults
•Document Reviews
•Additional Testing
•Administrative QA Review
Profile Qualify/Disqualify

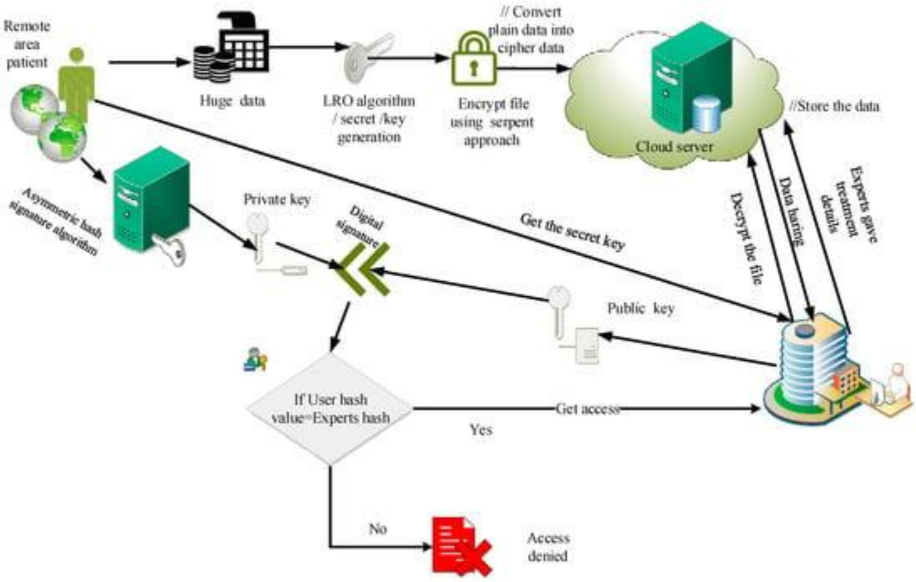
Note: MEPS (Military Entrance Processing Station)
Source: (National Research Council, 2006)

Figure 1. Process in medical evaluation of military personnel

This examination is also carried out during personnel recruitment, so that prospective military personnel are obtained with the best health conditions.

b. Data security

Data security provides benefits for an information system, through good data security management it can maintain data performance to remain stable, including application performance. In addition, it can also build user trust to use and utilize available data and information and is an effort to maintain data privacy (Nurul Wahda R. Kasad et al., 2023). Hospitals are one of the most important infrastructures that store, exchange, and use a lot of personal information. Therefore, with the large amount of confidential data that is stored for the purpose of patient care and activities, this sector has been considered a target, in addition to the potential value of personal health information having a higher value than the value of financial data (Almalawi et al., 2023). Figure 2 is a security system model that can be used by MCU systems for the military, because it provides protection for data flow and access procedures within it.


Remote area patient
Huge data
LRO algorithm / secret /key generation
// Convert plain data into cipher data
Encrypt file using serpent approach
Cloud server
//Store the data
Asymmetric hash signature algorithm
Private key
Digital signature
Get the secret key
Decrypt the file
Data haring
Experts gave treatment details
Public key
If User hash value=Experts hash
Get access
Yes
No
Access denied

Source: (Almalawi et al., 2023)

Figure 2. Security system that can be used for military MCU Information System

c. Conditions encountered

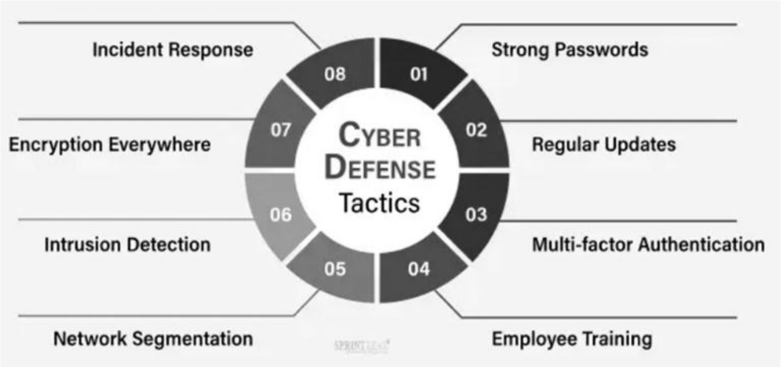
The MCU information system should have strong and reliable data security technology during its lifetime, so it is highly recommended to upgrade the system itself along with its devices and security. With awareness of the need for system security and its devices, concerns about cyber crime can be resolved with the best solution. Hospitals as users of the MCU information system must always be aware of the various potential threats that can occur with various solutions. Risk management planning for cyber security is a component that is no less important in protecting the system because it can help in assessing, identifying, and reducing the risk of attacks and damage that can occur. The implementation of various cyber security risk management strategies must be carried out comprehensively and continuously to protect the MCU information system and its devices. (Wright, 2023). This will impact the entire spectrum of the healthcare sector as it results in increased cybersecurity risks such as ransomware, phishing, and also distributed denial-of-service. (He et al., 2021). Because the MCU information system in military hospitals is closely related to military personnel data which is ultimately also related to the country's military strength data, data security is one of the main priorities. In Table 1, we can see several forms of attacks that have occurred against health data, and these attacks have caused losses that are not only internal. From some of these attacks, there are also several actions taken after the attack occurred, so that they can be a reference solution in dealing with similar attacks..

Table 1. Cyber crime attacks that have occurred based on previous research

References	Issues	Impacts	Actions
(Mishra, 2024)	- There was a ransomware attack in 2020 targeting the Brno University Hospital in the Czech Republic. - There was a breach that occurred in May 2021 directed at the Health Service of Ireland (HSE)	- This attack on cyberspace eventually spread outside the hospital - Supply chains for biomedicals are being disrupted covering a wider area.	In investing, efforts are made not only on the advanced technology available to detect and mitigate cyber-attacks but also on training and preparing staff to be able to deal with incidents that may occur
(Riggi, 2024)	Crimes of data theft and attacks on healthcare providers and third-party providers.	Hospitals cannot solve problems independently.	Carrying out international cooperation consisting of hackers and ransomware groups.
(WHO, 2024)	- During the COVID-19 pandemic, the infrastructure in health information technology (IT) has become a target for many cyber attacks, thus becoming an obstacle for hospital activities in providing timely health services when they are needed. - Disinformation, is an information weapon that can cause negative effects such as disharmony, disputes, and distrust in a particular target such as Public Health Institutions, government, law enforcement, scientific experts, and even the private sector.	- Recovery efforts made for IT systems and also retrieving stolen data, then must pay a large ransom. - Become an ideological or political agenda for a broader and long-term direction, or can also be for economic gain, so that some disinformation messages are deliberately created and distributed professionally.	Make efforts to increase cyber-maturity.

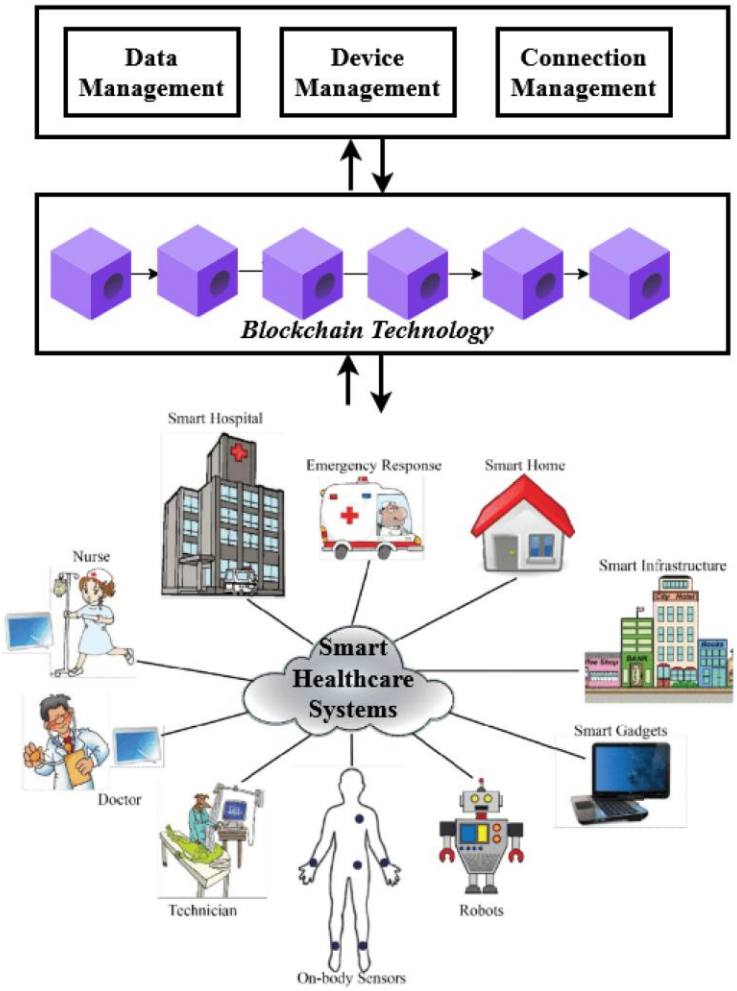
d. Efforts to overcome

From previous research, various methods are used to secure the system and its devices, especially data and information. In addition to planning risk management, a culture of awareness of cybersecurity is an important aspect in efforts to reduce the risk of cyber-attacks that must be instilled in all parts of the organization. The increasing use of technology, which is also combined with the nature of the complex MCU information system and integrated infrastructure, causes vulnerability to various cyber threats. Thus, it is very important to develop a mitigation strategy, equipped with risk management, although there are still some weaknesses that must also be considered, efforts to minimize the effects of attacks and attack predictions have been accommodated (Wright, 2023). In Figure 3, we can see the actions that can be taken to deal with attacks from cybercrime and solutions that can be prepared before and/or if an attack has already occurred.



Source: (Yanthan, 2023)
Figure 3. Actions to address cyber crime attacks

However, information systems in the military environment must have their own specifications for their security methods. For example, if using a cryptographic algorithm, it does not use a common algorithm that already exists, but there are special specifications, such as a multi-level encryption-description process. In addition, building a method with special military specifications to support data security, is an innovation that can be done so that the fulfillment of military data security such as health data can be done more optimally and effectively. Figure 4 is a form of the architecture layer for cyber security in a healthcare system that already has a security method using blockchain technology. This method can also be used in MCU information systems but still requires additional security which is the next innovation, especially in the military field.



Source: (Selvarajan & Mouratidis, 2023)

Figure 4. Architectural layer model for cyber security in healthcare systems

CONCLUSION

However, information systems in the military environment must have their own specifications for their security methods. For example, if using a cryptographic algorithm, it does not use a common algorithm that already exists, but there are special specifications, such as a multi-level encryption-description process. In addition, building a method with special military specifications to support data security, is an innovation that can be done so that the fulfillment of military data security such as health data can be done more optimally and effectively. Figure 4 is a form of the architecture layer for cyber security in a healthcare system that already has a security method using blockchain technology. This method can also be used in MCU information systems but still requires additional security which is the next innovation, especially in the military field.

REFERENCES

Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing Security of Healthcare Data for a Modern Healthcare System. *Sensors*, *23*(7), 1–18. https://doi.org/10.3390/s23073612

Andriani, W. (2022). Penggunaan Metode Sistematik Literatur Review dalam Penelitian Ilmu Sosiologi. *Jurnal PTK Dan Pendidikan*, *7*(2). https://doi.org/10.18592/ptk.v7i2.5632

Crisnaldy, A. (2021). Literature Review (Metodologi Penelitian). *ReseachGate. Net*, *May*, 1–22.

Grandis G. D., L., Girsang, E., Sari Mutia, M., & Napiah Nasution, A. (2022). Evaluation Of Development Of Medical Check-Up Services At Putri Hijau Hospital. *International Journal of Health and Pharmaceutical (IJHP)*, *2*(2), 367–379. https://doi.org/10.51601/ijhp.v2i2.56

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research*, *23*(4), 1–18. https://doi.org/10.2196/21747

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, *17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Mishra, V. (2024). *Cyberattacks on healthcare: A global threat that can't be ignored*. UN. https://news.un.org/en/story/2024/11/1156751

National Research Council. (2006). *Assessing Fitness for Military Enlistment: Physical, Medical, and Mental Health Standards* (p. 264). https://nap.nationalacademies.org/read/11511/chapter/4

Nurul Wahda R. Kasad, Deden Witarsyah Jacob, & Ramdhan Nugraha. (2023). Data Security Management and Audit of Healthcare Data: A Case Study of SISPEC19 Project. *Asia Pacific Journal of Information System and Digital Transformation*, *1*(01), 33–52. https://doi.org/10.61973/apjisdt.v101.4

Pardamean, B., Louis, S., & Setyaningrum, L. (2012). Designing Medical Checkup Information System for the Navy Hospitals. *International Journal of Biology and Biomedical Engineering*, *6*(27), 105–113.

Riggi, J. (2024). *A Look at 2024's Health Care Cybersecurity Challenges*. https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges

Selvarajan, S., & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Scientific Reports*, *13*(1), 1–22. https://doi.org/10.1038/s41598-023-34354-x

WHO. (2024). *WHO-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies*. https://www.who.int/news/item/06-02-2024-who-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, *4*(4), 17–27. https://doi.org/10.61093/hem.2023.4-02

Yanthan, N. (2023). *Prevent Cyber Attacks: Strategies to Protect Your Digital Assets*. https://www.sprintzeal.com/blog/prevent-cyber-attacks