International Journal of Humanities, Social Sciences and Business (INJOSS) e-ISSN: 2962-6781
Vol. 4 No. 1 2025, page 416-425

DATA SECURITY IN COMPUTERS: AN INTRODUCTION TO THE CONCEPT OF ENCRYPTION

Loso Judijanto *
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Al-Amin
Universitas Airlangga, Surabaya, Indonesia
al.amin-2024@feb.unair.ac.id

Abstract

Encryption is a vital process in computer data security that converts open information into encrypted text to protect it from unauthorised access. The process relies on the use of complex algorithms and decryption keys that ensure that only authorised parties can access the information. Encryption security is crucial in this digital age to maintain privacy and protect the information assets of organisations and individuals during data storage and transmission. However, the implementation of this security faces challenges such as secure key management, selection of robust and efficient algorithms, and complying with regulations related to the use of encryption technology. With continuous development and multi-stakeholder engagement, encryption-based data security can be continuously strengthened to deal with dynamic cyber threats.
Keywords: Data Security, Computer, Encryption.

INTRODUCTION

In the ever-evolving digital age, data is becoming a very valuable asset for individuals and organisations. Data can be personal information, state secrets, financial data, and intellectual property, all of which have economic, social, or political value. With the increasing volume of data generated and stored in computer systems and networks, there are serious data security risks. (Yu et al., 2021). These risks can stem from cyberattacks, identity theft, data leakage, or unauthorised access to sensitive data. Data security is an important issue that must be considered to protect digital assets from cybersecurity threats.

Data security acts as the backbone of the digital economy, holding everything from users' personal information to business secrets that if leaked can be financially and reputationally damaging. Increased online transactions, social media usage, and electronic data recording demand stricter data protection to avoid identity theft, financial fraud, and unauthorised dissemination of personal information. (Song et al., 2021). The vulnerability of data to cyberattacks forces organisations and individuals to adopt strong security practices, including the use of encryption, two-factor authentication, and transparent privacy policies to ensure data remains safe and secure. (Joshi et al., 2022).

Failure to protect data security not only results in direct economic losses for companies through fines and damages, but also damages user trust, which can ultimately affect business survival. In a continuously connected society, the risk of data leakage increases, making effective security practices even more important (Aslan et al., 2023). Effective data protection enables individuals and businesses to leverage technological advancements with confidence, drive innovation, and maintain information integrity in an ever-changing digital environment. Hence, investment in data security is not only a corporate ethical responsibility, but also a strategic investment in reputation and business sustainability (Li & Liu, 2021).

Cybercrime is one of the most significant threats in cyberspace, where perpetrators can exploit security gaps to access, alter, or destroy information without authorisation. Therefore, security measures that can effectively protect data are required. One of the most powerful methods in maintaining data confidentiality and integrity is encryption. (Daniel et al., 2021).

Encryption is the process of converting information or data into a secret code (cipher) to protect that data from unauthorised access. It uses an encryption algorithm and an encryption key to convert readable data into a format that cannot be easily interpreted without a decryption key. This principle ensures that only individuals or entities that have the decryption key can read and understand the data. (Adee & Mouratidis, 2022).

Encryption enables the secure transmission of data over insecure networks, such as the internet, and provides a means to maintain the confidentiality and privacy of information. Encryption is used in a wide range of applications, from email security, to online banking transactions, to confidential communications between individuals or government bodies. (Vegesna, 2023).

While encryption offers a high level of protection, its use and implementation itself faces challenges. Firstly, weak encryption algorithm selection or improper implementation can lead to vulnerabilities. Second, ineffective encryption key management can allow data leakage. Third, increasingly sophisticated cyber-attacks can attempt to break encryption through a variety of methods, including brute force computation or exploitation of software vulnerabilities. (Kumar et al., 2021).

With cybersecurity threats growing, it is important to understand and implement encryption as part of a comprehensive data security strategy. A sound knowledge of encryption concepts and awareness of potential security risks is an important first step in protecting digital assets in an increasingly connected world.

Research Methods

The study in this research uses the literature method. The literature research method is a study approach conducted through a review and analysis of various previously published sources of information, such as books, journal articles, research

reports, and other documents relevant to the research topic. This process involves searching, collecting, and evaluating literature to obtain theoretical frameworks, support hypotheses, or answer research questions. (Syafril & Erlina, 2018); (Alaslan, 2022). Through this method, researchers can identify trends, patterns, opinions, and theories that have developed in a particular topic, as well as uncover research gaps that can still be explored. The literature research method allows researchers to build arguments or recommendations based on existing scientific evidence and discussions, so it is very instrumental in the development of new knowledge. (Suyitno, 2021); (Adlini et al., 2022).

Results and Discussion

Encryption and How it Works

Encryption is the process of converting data into a code or other form that cannot be read without having the key to decrypt it. Its main purpose is to protect the confidentiality of data by preventing unauthorised access during data transmission or while stored. (Thabit et al., 2021). This technique is widely used in various fields such as digital communications, banking, and internet security services to secure information from spies or hackers. Encryption ensures that only people or systems with the right decryption key can access the original data, making it an important tool in maintaining privacy and information security (Wu et al., 2022). (Wu et al., 2022).

The working mechanism of encryption starts with the use of an encryption algorithm that converts the original data, called plain text, into encrypted text through a process called encryption. The algorithm utilises a unique encryption key, which when applied to the plaintext, produces an unreadable output. (Shen et al., 2021). To decrypt the encrypted text and restore it to its original format, a decryption key is required, which can be the same or different from the encryption key depending on the type of encryption used: symmetric encryption (where the encryption and decryption keys are the same) or asymmetric encryption (where two separate keys are used). This process ensures that only recipients who have the right decryption key can access and read the data, thus protecting the information from unwanted access (Agyekum et al., 2014). (Agyekum et al., 2021).

In the world of encryption, there are two main types of keys used: symmetric keys and asymmetric keys, and they operate in different ways.

Symmetric Key is an encryption method where the same key is used for both encryption and decryption of data. This means that the remitter and receiver of the message must have identical copies of the key in order to effectively encrypt and decrypt the message. Symmetric keys must be transferred over a secure channel as their disclosure to unauthorised parties can compromise the security of the communication. Popular symmetric encryption algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). The advantage of symmetric keys is their relatively

fast processing, which makes them ideal for encryption of large amounts of data. (Prajapati & Shah, 2022)..

Asymmetric Key, or public key encryption, on the other hand, uses a pair of keys: one public key that can be freely shared and one private key that must be kept secret. The public key is used to encrypt the message, while the private key is used to decrypt it. This method solves the key transfer problem present in symmetric encryption, as only the private key must be kept secure, while the public key can be openly distributed. Well-known public-key encryption algorithms are inclusive of RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and ElGamal (Unal et al., 2021).

Asymmetric key operation mechanisms include processes such as digital signature and key exchange. For example, in the case of digital signature, the sender can "sign" a document with their private key, and anyone with the public key can verify that the signature is valid. For key exchange, protocols such as Diffie-Hellman allow two parties to agree on a common symmetric key that is secure against eavesdropping, even if they communicate over an insecure channel. (Abhishek et al., 2022)..

The choice between using symmetric and asymmetric keys often depends on the application context and the need for security. Asymmetric keys tend to be more secure and flexible as the private key does not need to be transferred over the network. However, encryption and decryption operations with asymmetric keys are slower than with symmetric keys, which makes them less ideal for large-scale data encryption. (Singh & Kumar, 2024). Therefore, often the use of both is combined in practice: the asymmetric key is used for the beginning of the communication and the exchange of the symmetric key that will be used for that communication session.

The Importance of Encryption for Data Security

Encryption is the process of securing data by converting information into a form that cannot be read by unauthorised parties, thus playing a critical role in privacy protection and data security. In this digital age, data can be so sensitive - from personal information to business secrets - that if it falls into the wrong hands, it can lead to huge financial losses, privacy breaches, and even national security risks. Through encryption, data is converted into ciphertext, which can only be reinterpreted (decrypted) by a party in possession of the appropriate decryption key. (Munjal & Bhatia, 2023).

Encryption offers protection to data either while it is stored (called encryption at rest) or while it is being transmitted over a network (called encryption in transit). In the case of encryption at rest, data stored on servers, computers, or mobile devices, such as documents, images, and databases, is encrypted to protect it from illegal access in the event of physical theft or cyber attack. (Abdullah et al., 2022). When data is encrypted in transit over the internet or other networks, it is protected from eavesdropping or capture by snoopers who may try to obtain sensitive data during such transfers.

In the business and industrial sector, encryption is an important layer of defence in maintaining the confidentiality and integrity of corporate data. Encryption not only protects information from theft by competitors but also helps in meeting compliance standards such as GDPR (General Data Protection Regulation) in the European Union, HIPAA (Health Insurance Portability and Accountability Act) in the United States, and various other privacy regulations. Failure to protect the data of its customers and clients can cause businesses to face fines, loss of customer trust, and irreparable reputational damage (Ali et al., 2024). (Ali et al., 2024).

At the individual level, encryption helps in ensuring the privacy and security of online communications. Given the possibility that internet service providers (ISPs), governments, and other third parties may try to monitor or record online activities, encryption such as that used in VPNs (Virtual Private Networks), secure messaging apps, and encrypted browsing technologies offer an additional layer of security. (Thummisetti & Atluri, 2024). It helps ensure freedom of speech and protects personal information from commercial exploitation or unwanted surveillance. In this information age, encryption is an essential tool in maintaining personal privacy and maintaining control over our personal information. (Ramachandra et al., 2022).

Then, realising that technological developments always go hand in hand with improved techniques that cyber criminals can use to access unencrypted data. The increase in cyber-attacks, phishing and ransomware are examples of digital threats that continue to adapt and attempt to overcome security barriers, including encryption. (Awadallah et al., 2021).. Therefore, encryption is not only important, but must be constantly updated to keep up with the latest threat trends, ensuring that the encryption methods used are reasonable and effective against evolving hacking techniques.

In an increasingly connected world, encryption is no longer an option but a necessity. For individuals, personal data security can ensure financial security and privacy. Meanwhile, for corporations, encryption can counteract potential economic losses caused by data leaks. This discussion is not only limited to the use of encryption in digital technology, but also in understanding the nature and skills in utilising it responsively; for example, using strong passwords, keeping decryption keys secure, and understanding the security protocols implemented by the applications and services we use. (Lv et al., 2021).

As such, encryption is a central element in maintaining data security in the digital age. It is a bulwark in protecting information from external and internal threats, creating trust between parties involved in digital communication, and ensuring compliance with strict privacy standards. In the future, with technological advancements such as quantum computing potentially threatening current encryption methods, the importance of encryption will remain relevant and will continue to grow. That is why we must continue to invest time and resources into developing stronger encryption

techniques and understanding how best to implement them in our daily activities, both professionally and personally.

Challenges in Encryption Implementation

The implementation of encryption does have a number of challenges to face, ranging from technical to social and political aspects.

Encryption deployments often face the challenge of striking a balance between strong security and user convenience. Complicated and strong encryption usually requires users to remember complex passwords or perform additional steps for verification, which can lead to inconvenience and resistance from users. Conversely, if the process is too simple, it may reduce the level of security offered. This challenge is compounded by the diverse range of users with different levels of digital literacy using encryption technology. (Alruily et al., 2021)..

Encryption key management is one of the most important yet challenging aspects of encryption. Encryption keys must be kept confidential, stored in a secure location, and managed properly to prevent them from falling into the wrong hands. Errors in key management can result in losing access to encrypted data or worse, make the data open to unauthorised parties. This challenge also includes secure key distribution as well as periodic key changes without disrupting service or data accessibility. (Zuo et al., 2021).

Encryption can increase the computational load that the system has to handle, potentially degrading the overall performance. Especially on resource-constrained systems or applications that require fast response times, encryption performance must be matched to system capacity. Developers must find encryption methods that are not only secure, but also resource-efficient, so as to minimise performance degradation and ensure that the application or service continues to run smoothly. (Sohal & Sharma, 2022).

Regulations and policies in different countries or regions can pose a challenge to the adoption of encryption. Some governments have provisions that restrict the use of encryption or require institutions to provide a backdoor for law enforcement purposes. Such rules can present ethical and technical dilemmas for IT companies and policymakers who must guarantee user privacy while complying with local regulations. These regulatory challenges also involve navigating a changing legal environment and often ambiguity in the interpretation of applicable rules (Das et al., 2021).

Meeting these challenges requires a holistic and continuous approach to encryption technology development, as well as the engagement of various parties, including users, developers, enterprises, and government agencies, to create a secure and reliable digital environment.

Conclusion

Data security in the world of computing is important and inevitable, especially in today's digital era where data is one of the most important assets. Encryption comes as an answer to the need for data protection. Through the concept of encryption, data that was originally in clear text is converted into encrypted text that cannot be read without the right decryption key. This process provides a strong layer of protection, securing data from unauthorised access, either during storage or transmission. Encryption is therefore the foundation for building data security and privacy for individuals and organisations in various computing applications.

However, implementing encryption is not without its challenges. These challenges include secure key management, selection of the right encryption algorithm, and the need for a balance between encryption strength and system efficiency. On the other hand, the existence of regulations and policies in some areas that govern the use of encryption adds to the complexity of its implementation. However, with the continuous development of technology and the involvement of various parties in ensuring encryption security, data security in computing can be continuously improved, ensuring that data remains safe amidst evolving cyber threats.

References

Abdullah, N., Zakaria, N., Halim, A. A., & ... (2022). A theoretical comparative analysis of DNA techniques used in dna based cryptography. *Journal of ...*, *Query date: 2024-11-05 18:55:17.* https://jssm.umt.edu.my/wp-content/uploads/sites/51/2022/06/Article-14-JSSM-Volume-17-Number-5-May-2022.pdf

Abhishek, Tripathy, H., & Mishra, S. (2022). A succinct analytical study of the usability of encryption methods in healthcare data security. *Next Generation Healthcare Informatics*, *Query date: 2024-11-05 18:55:17.* https://doi.org/10.1007/978-981-19-2416-3_7

Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *Query date: 2024-11-05 18:55:17.* https://www.mdpi.com/1424-8220/22/3/1109

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Qualitative Research Methods of Literature Study. *Edumaspul: Journal of Education*, *6*(1), 974-980. https://doi.org/10.33487/edumaspul.v6i1.3394

Agyekum, K., Xia, Q., Sifah, E., & ... (2021). A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. *IEEE Systems ...*, *Query date: 2024-11-05 18:55:17.* https://ieeexplore.ieee.org/abstract/document/9442931/

Alaslan, A. (2022). *QUALITATIVE RESEARCH METHODS*. *Query date: 2024-05-25 20:59:55.* https://doi.org/10.31237/osf.io/2pr4s

Ali, S., Wadho, S., Yichiet, A., Gan, M., & Lee, C. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. *Egyptian Informatics Journal*, *Query date: 2024-11-05 18:55:17.* https://www.sciencedirect.com/science/article/pii/S1110866524000823

Alruily, M., Shahin, O., Al-Mahdi, H., & Taloba, A. (2021). Asymmetric DNA encryption and decryption technique for Arabic plaintext. *... and Humanised Computing*, *Query date: 2024-11-05 18:55:17.* https://doi.org/10.1007/s12652-021-03108-w

Aslan, Ö., Aktuğ, S., Ozkan-Okay, M., Yilmaz, A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *Query date: 2024-11-05 18:55:17.* https://www.mdpi.com/2079-9292/12/6/1333

Awadallah, R., Samsudin, A., Teh, J., & ... (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *IEEE Access*, *Query date: 2024-11-05 18:55:17.* https://ieeexplore.ieee.org/abstract/document/9420703/

Daniel, A., Shaba, S., Momoh, M., & ... (2021). A computer security system for cloud computing based on encryption technique. *Computer Engineering ...*, *Query date: 2024-11-05 18:55:17.* https://www.academia.edu/download/87355012/222.pdf

Das, M., Tao, X., & Cheng, J. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. *Automation in Construction*, *Query date: 2024-11-05 18:55:17.* https://www.sciencedirect.com/science/article/pii/S0926580521001333

Joshi, B., Joshi, B., Mishra, A., Arya, V., Gupta, A., & ... (2022). A comparative study of privacy-preserving homomorphic encryption techniques in cloud *computing. ... and Computing ...*, *Query date: 2024-11-05 18:55:17.* https://www.igi-global.com/article/a-comparative-study-of-privacy-preserving-homomorphic-encryption-techniques-in-cloud-computing/309936

Kumar, S., Karnani, G., Gaur, M., & ... (2021). Cloud security using hybrid cryptography algorithms. *2021 2nd International ...*, *Query date: 2024-11-05 18:55:17.* https://ieeexplore.ieee.org/abstract/document/9445377/

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *Query date: 2024-11-05 18:55:17.* https://www.sciencedirect.com/science/article/pii/S2352484721007289

Lv, Z., Qiao, L., Hossain, M., & Choi, B. (2021). Analysis of using blockchain to protect the privacy of drone big data. *IEEE Network*, *Query date: 2024-11-05 18:55:17.* https://ieeexplore.ieee.org/abstract/document/9354924/

Munjal, K., & Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex &Intelligent Systems*, *Query date: 2024-11-05 18:55:17.* https://doi.org/10.1007/s40747-022-00756-z

Prajapati, P., & Shah, P. (2022). A review on secure data deduplication: Cloud storage security issue. *... of King Saud University-Computer and Information ...*, *Query date: 2024-11-05 18:55:17.* https://www.sciencedirect.com/science/article/pii/S1319157820305140

Ramachandra, M., Rao, M. S., Lai, W., & ... (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. *... Cognitive Computing*, *Query date: 2024-11-05 18:55:17.* https://www.mdpi.com/2504-2289/6/4/101

Shen, J., Yang, H., Vijayakumar, P., & ... (2021). A privacy-preserving and untraceable group data sharing scheme in cloud computing. *... and Secure Computing*, *Query date: 2024-11-05 18:55:17*. https://ieeexplore.ieee.org/abstract/document/9319526/

Singh, S., & Kumar, D. (2024). Enhancing cyber security using quantum computing and artificial intelligence: A review. *Algorithms*, *Query date: 2024-11-05 18:55:17*. https://www.researchgate.net/profile/Shoumya-Singh/publication/381519152_Enhancing_Cyber_Security_Using_Quantum_Computing_and_Artificial_Intelligence_A_Review/links/66725da6b769e7691940fdc5/Enhancing-Cyber-Security-Using-Quantum-Computing-and-Artificial-Intelligence-A-Review.pdf?utm_source=www.thedailyqubit.com&utm_medium=referral&utm_campaign=the-daily-qubit

Sohal, M., & Sharma, S. (2022). BDNA-A DNA inspired symmetric key cryptographic technique for secure cloud computing. *... of King Saud University-Computer and Information ...*, *Query date: 2024-11-05 18:55:17*. https://www.sciencedirect.com/science/article/pii/S1319157818303999

Song, H., Li, J., & Li, H. (2021). A cloud secure storage mechanism based on data dispersion and encryption. *IEEE Access*, *Query date: 2024-11-05 18:55:17*. https://ieeexplore.ieee.org/abstract/document/9411835/

Suyitno. (2021). *QUALITATIVE RESEARCH METHODS CONCEPTS, PRINCIPLES AND OPERATIONS*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31219/osf.io/auqfr

Syafril, S., & Erlina, N. (2018). *Preparing Interview Protocols, Selecting Informants and Probing in Qualitative Research*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31219/osf.io/pvsh3

Thabit, F., Alhomdy, S., Al-Ahdal, A., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions...*, *Query date: 2024-11-05 18:55:17*. https://www.sciencedirect.com/science/article/pii/S2666285X21000133

Thummisetti, B., & Atluri, H. (2024). Advancing healthcare informatics for empowering privacy and security through federated learning paradigms. *... of Sustainable Development in Computing ...*, *Query date: 2024-11-05 18:55:17*. https://ijsdcs.com/index.php/ijsdcs/article/view/434

Unal, D., Al-Ali, A., Catak, F., & Hammoudeh, M. (2021). A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. *Future Generation Computer...*, *Query date: 2024-11-05 18:55:17*. https://www.sciencedirect.com/science/article/pii/S0167739X21002454

Vegesna, V. (2023). A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments. *International Journal of Management, Technology ...*, *Query date: 2024-11-05 18:55:17*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4612537

Wu, X., Zhang, Y., Wang, A., Shi, M., Wang, H., & ... (2022). MNSSp3: Medical big data privacy protection platform based on Internet of things. *Neural Computing and ...*, *Query date: 2024-11-05 18:55:17*. https://doi.org/10.1007/s00521-020-04873-z

Yu, K., Tan, L., Yang, C., Choo, K., & ... (2021). A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings. *IEEE Internet of ..., Query date: 2024-11-05 18:55:17.* https://ieeexplore.ieee.org/abstract/document/9600469/

Zuo, Y., Kang, Z., Xu, J., & Chen, Z. (2021). BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. *International Journal of ..., Query date: 2024-11-05 18:55:17.* https://doi.org/10.1177/1550147721999616