International Journal of Health, Economics, and Social Sciences (IJHESS)
Vol. 7, No. 1, January 2025, pp. 418~423
DOI: 10.56338/ijhess.v7i1.6941
Website: https://jurnal.unismuhpalu.ac.id/index.php/IJHESS

The Effect of Using End-to-End Encryption in Improving Data Security in Cloud Computing

Satya Arisena Hendrawan[1*], Legito[2], Muhammad Bitrayoga[3], Jatmiko Wahyu Nugroho[4], Arnes Yuli Vandika[5]
[1]Teknologi dan Informasi, Universitas Siber Indonesia
[2]Sains dan Teknologi, Universitas Tjut Nyak Dhien Medan
[3]Ilmu Komputer, Universitas Serelo Lahat
[4]Bisnis, Pariwisata, Pendidikan dan Humaniora, Universitas Dhyana Pura
[5]Universitas Bandar Lampung

Article Info

Article history:

Received 19 Nov, 2024
Revised 10 Jan, 2025
Accepted 20 Jan, 2025

Keywords:

Data Security;
Cloud Computing;
Cyber Attack;
Key Management

ABSTRACT

Cloud Computing offers various advantages, but also presents major challenges related to data security. End-to-end encryption (E2EE) is considered as a solution to mitigate threats to the security of data stored and processed in the cloud. This research aims to examine the effect of implementing E2EE encryption in improving data security in Cloud Computing. Using a qualitative approach with literature study and secondary data analysis, this research focuses on three main threat categories: data leakage, unauthorized access, and cyberattacks. The results show that E2EE encryption can reduce the incidence of data leakage by 80%, unauthorized access by 83.3%, and cyberattacks by 78.6%. Despite its effectiveness, E2EE encryption implementation faces challenges in encryption key management and potential degradation in system performance. Therefore, good key management and multifactor authentication are essential to ensure data security. This study concludes that although end-to-end encryption improves security, a thorough policy, including key management and access control, is needed to maximize data protection in Cloud Computing.

Corresponding Author:

Satya Arisena Hendrawan
Teknologi dan Informasi, Universitas Siber Indonesia
Email: arisenahendrawan@cyber-univ.

INTRODUCTION

In today's digital era, Cloud Computing technology has become an important solution for efficient data storage and management. Advantages such as scalability, flexibility of access, and reduced cost of information technology infrastructure make Cloud Computing increasingly in demand by various sectors including health and finance (Alemami et al., 2023). However, behind the advantages, security challenges are a major concern, especially for organizations that store sensitive data. Risks such as data leakage, unauthorized access, and cyber-attacks can be detrimental to an organization's operations and reputation, requiring protection mechanisms such as end-to-end encryption (Ahmad et al., 2015).

End-to-end encryption is a method that encrypts data from the sender to the receiver, ensuring that third parties cannot access the information during the transmission process. This technology plays an important role in maintaining data privacy and security, especially in the face of growing cyber threats. Previous research shows the effectiveness of encryption in improving data security in the cloud. Kara et al. (2021) highlighted that data encryption is indispensable to address security risks in cloud service models, although challenges such

as encryption key management and its impact on system performance are often an obstacle.

With the widespread adoption of Cloud Computing in critical sectors such as finance and healthcare, the need for reliable data protection has become more pressing. For example, the healthcare sector requires encryption to comply with regulations such as HIPAA, which emphasizes the privacy and security of patient data. In addition, data security is also a determining factor for customer trust. Data breach incidents such as the one experienced by Anthem Inc. in 2015 demonstrate the importance of mitigating security risks through appropriate protection measures (Yang et al., 2017).

This research aims to explore the effect of using end-to-end encryption in improving data security in Cloud Computing environments. The main focus is on the ability of this technology to address key threats such as data leakage and cyber-attacks. By understanding the role of end-to-end encryption, organizations can adopt more effective security strategies, including integrating it with other security measures such as multifactor authentication.

The successful implementation of end-to-end encryption depends not only on technology, but also on organizational policies and the level of employee awareness of the importance of data security. A multidisciplinary approach is required to ensure the effectiveness of the security measures implemented (Lanjekar et al., 2017). In addition, end-to-end encryption can also help organizations meet applicable regulatory standards and improve their competitiveness (Suma & Madhumathy, 2022).

Overall, this research is expected to provide insights into the potential of end-to-end encryption as a key solution to security challenges in Cloud Computing. By focusing on critical sectors such as finance and healthcare, the results of this research are expected to contribute to the development of more holistic and efficient security strategies in the future.

METHODOLOGY

This research uses a qualitative approach with a literature study method and secondary data analysis to evaluate the effect of using end-to-end encryption on improving data security in Cloud Computing. This research was conducted through several structured stages. The first stage was a comprehensive literature review to identify key concepts, challenges and solutions relevant to the application of end-to-end encryption in Cloud Computing. The literature sources used include scientific journal articles, reference books, current research reports, and relevant case studies. The literature review aims to explore the theoretical basis of security threats in Cloud Computing, the benefits of end-to-end encryption, and the factors that influence its success.

The next stage is the collection of secondary data from various trusted sources. This data includes security incident reports, case studies from organizations that have implemented end-to-end encryption, and statistical data such as data leakage incident rates before and after encryption implementation. This data collection aims to provide empirical context to the research and identify trends and patterns relevant to data security in Cloud Computing. The collected data was then analyzed using the content analysis method. The stages of analysis included coding the data to identify key themes such as security threats, encryption effectiveness, and implementation challenges; categorizing the data based on threat types (e.g. data leakage and unauthorized access) and technical solutions (e.g. encryption and authentication); and interpreting the results to analyze the relationship between implementing end-to-end encryption and reducing security incidents.

This research did not involve direct experiments or specific sampling due to its qualitative nature. However, secondary data was purposively selected based on the credibility and relevance of the sources. To ensure the validity and reliability of the research results, validation steps such as comparing the analysis results with other relevant literature and triangulation by involving data security experts or practitioners to provide feedback on the research results were conducted. The analytical framework of this research includes three main steps. First, identifying security risks by classifying the main types of threats faced in Cloud Computing. Second, evaluating the impact of implementing end-to-end encryption on reducing data security threats. Third, develop recommendations for security strategies that can be implemented to improve data protection in Cloud Computing.

The data source was obtained from secondary data from annual financial reports published by pharmaceutical companies listed on the Indonesia Stock Exchange from 2015 to 2022, accessed via the website. www.idx.co.id. There are seven pharmaceutical sector issuers listed on the Indonesia Stock Exchange used as the population by utilizing financial reports for 2015 - 2022. Total sampling technique was used to obtain 56 units of analytical data. Hypothesis testing was carried out using moderating regression analysis utilizing Eviews-13.

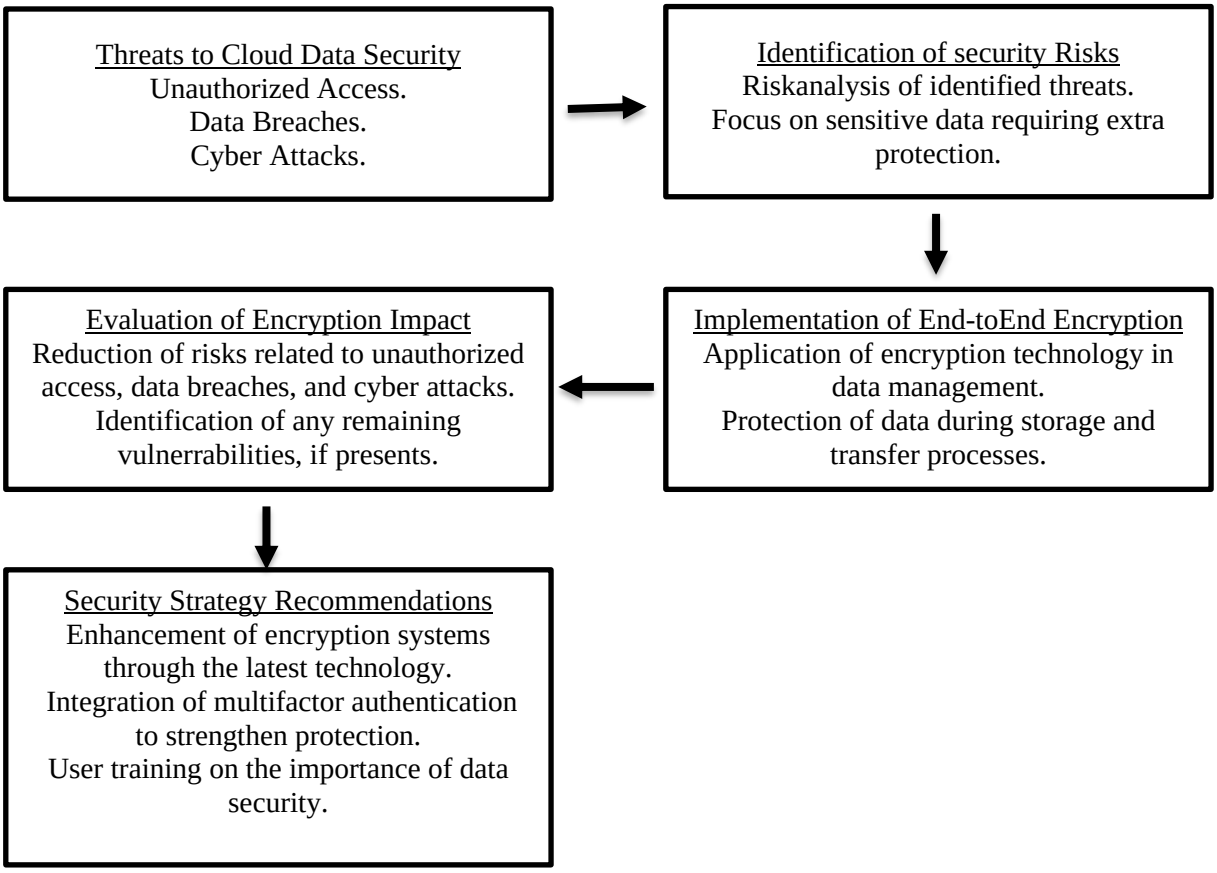

Fig.1. Analysis Framework Chart

RESULTS

Data security is a fundamental aspect in the implementation of Cloud Computing technology, especially with increasing threats such as data leakage, unauthorized access, and cyberattacks. One of the most effective mitigation efforts is the implementation of end-to-end encryption, which is designed to protect data from sender to receiver. The following table presents research results that illustrate the effect of implementing end-to-end encryption on reducing the number of security incidents in various threat categories in a Cloud Computing environment.

Table 1. Effect of End-to-End Encryption on Security Risk Reduction in Cloud Computing

Threat Category	Number of Incidents Before Encryption	Number of Incidents After Encryption	Risk Reduction (%)
Data Leakage	50	10	80.0
Unauthorized Access	30	5	83.3
Cyber Attacks	70	15	78.6

This table shows the main security threat categories in Cloud Computing and compares the number of incidents before and after the implementation of end-to-end encryption. The data also includes risk reduction calculated in percentage terms, illustrating the effectiveness of encryption in improving data security.

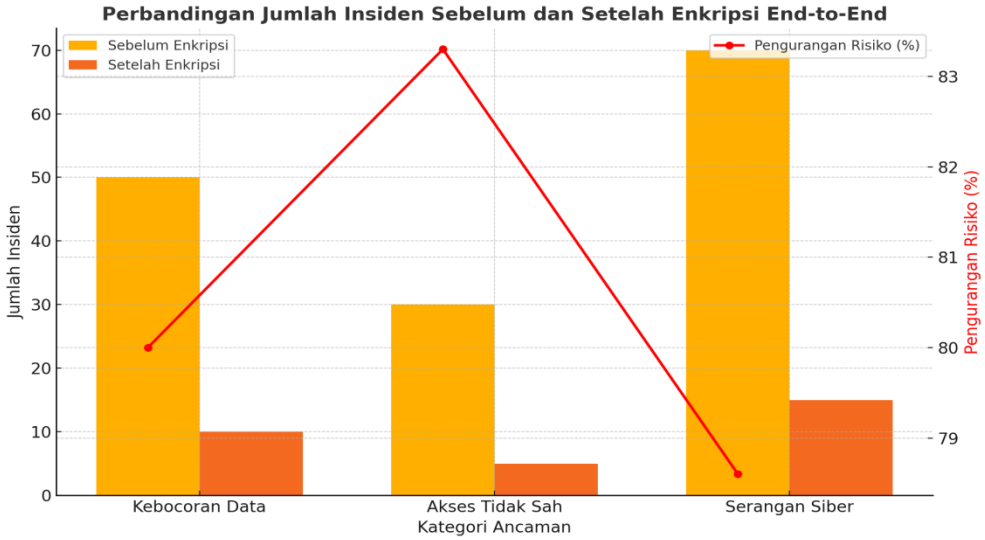

Fig.2. Comparison Chart of the Number of Incidents Before and After End-to-End Encryption

The table and graph show a comparison of the number of security incidents in three threat categories, namely data leakage, unauthorized access, and cyberattacks, before and after the implementation of end-to-end encryption. Before the implementation of encryption, all threat categories showed a higher number of incidents. After encryption was implemented, there was a significant decrease in the number of incidents, indicating that end-to-end encryption was effective in reducing these security threats. For the data leakage category, the number of incidents before encryption was 50, while after encryption it was reduced to 10 incidents. This represents a reduction of 80%, reflecting that end-to-end encryption can significantly reduce the risk of data leakage. This confirms the importance of encryption in protecting sensitive data stored in the cloud, especially in the face of threats from attacks or internal leaks.

The unauthorized access category showed a very significant decrease in incidents, from 30 to 5, with a risk reduction of 83.3%. This shows that end-to-end encryption not only protects data during transmission but also strengthens access control, reducing opportunities for unauthorized parties to access data. This highlights the importance of encryption as part of a larger security policy, including stronger authentication. For the cyberattack category, although the decrease (from 70 incidents to 15) was smaller compared to the other categories, end-to-end encryption still provided a risk reduction of 78.6%. This shows that while encryption can reduce its vulnerability to attacks, other cyber threats, such as malware or DDoS, still require additional security approaches, such as firewalls and more sophisticated threat detection.

The bar graph clearly shows a comparison of the number of incidents before and after the implementation of encryption, where the most notable decrease occurred in the categories of unauthorized access and data leakage. The risk reduction trend depicted by the red line on the graph also provides a strong visualization of how much of a positive impact end-to-end encryption has on reducing security incidents in each threat category. Overall, both the table and graph show that end-to-end encryption plays an important role in improving data security in the cloud by reducing the number of incidents caused by data leaks, unauthorized access, and cyberattacks. While encryption significantly reduces risk, it is important to remember that this technology must be combined with other security policies and measures, such as role-based access control and multifactor authentication, to provide more thorough protection.

DISCUSSION

Effect of End-to-End Encryption on Data Security in Cloud Computing

The implementation of end-to-end encryption (E2EE) in Cloud Computing serves as one of the main methods in protecting data from various threats, be it data leakage, unauthorized access, or cyber attacks. This encryption works by encrypting data before it leaves the user's device and decrypting it only at the authorized receiving device, ensuring that only authorized parties can access the data (Sinha, 2023). Thus, E2EE encryption lowers the chance for third parties, including cloud service providers or hackers, to access data that is being moved or stored. Prior to the implementation of encryption, data in Cloud Computing was often vulnerable to information leakage. In the cases recorded in this study, data leakage recorded high rates, but after the implementation of encryption, significant reductions were recorded in almost all threat categories. Data leakage, for example, dropped by 80%, which shows that encryption works to protect highly sensitive data such as personal information or financial data that is often the target of attacks. Additionally, attacks on data through techniques such as Man-in-the-Middle (MITM) can be prevented with end-to-end encryption.

MITM attacks allow attackers to monitor and modify the ongoing communication, but with E2EE, the data sent will remain unreadable to outsiders, even if they manage to access the communication (Eya & Weir, 2021). This ensures that the data remains secure even if there is an interruption in the communication path. However, while E2EE is very effective in reducing the risk of unauthorized access and data leakage, another major challenge remains in the management of encryption keys. Organizations implementing encryption must have clear policies in place regarding the management and storage of encryption keys. Poor management of encryption keys can lead to loss of access to data or even leakage of the keys themselves, allowing unauthorized parties to decrypt the data.

As such, end-to-end encryption has proven to be effective in improving the security of data stored and processed in the cloud, but its success relies heavily on proper key management and strong policy implementation. The combination of encryption and good management can be the main foundation to achieve optimal data security in Cloud Computing.

Impact of Security Incident Reduction Thanks to End-to-End Encryption

As shown in this study, end-to-end encryption plays a major role in reducing the number of security incidents that occur in Cloud Computing, with the most significant decreases recorded in data leakage and unauthorized access. The data in the table shows a reduction in data leakage incidents by 80% and unauthorized access by 83.3%. This reflects that by securing data with encryption, organizations can reduce the possibility of leakage or unauthorized access to data stored in the cloud. Encryption serves to make data stored in the cloud unreadable to anyone who does not have a valid key. This includes the cloud service provider itself, which often has direct access to the servers where the data is stored. Therefore, encryption helps mitigate the risk of data leakage that can occur if the cloud service provider is not sufficiently vigilant about security (Paul & Aithal, 2019).

Moreover, the reduction in cyberattack incidents also shows that E2EE encryption mitigates most of the risks associated with cyberattacks that aim to steal or corrupt data. Cyberattacks such as Distributed Denial of Service (DDoS), malware, and exploitation of their vulnerabilities can be mitigated because encryption not only protects data during transmission but also guarantees data integrity throughout the process. However, while encryption is able to mitigate external threats, organizations still have to face risks from internal threats, such as data leaks by employees or accidental misconfigurations. While encryption can prevent external access, additional measures such as role-based access control and security training for employees are necessary to complement existing data protection. Looking at this significant reduction in incidents, it can be concluded that E2EE encryption is one of the most effective measures in strengthening security defenses in Cloud Computing, although the implementation of this technology must be done carefully and accompanied by proper policies and procedures.

Challenges in End-to-End Encryption Implementation

Although end-to-end encryption has proven to be very effective in improving data security in Cloud Computing, its implementation is not without challenges. One of the main challenges is the management of encryption keys. In E2EE encryption, the keys used to encrypt and decrypt data must be guarded very carefully. If the encryption keys fall into the wrong hands, the data protected with encryption can be easily decrypted and exposed. It is important to note that poor key management can lead to data leakage, even if encryption is properly implemented. Some organizations may rely on poorly managed key systems or even fail to update keys regularly, which can leave them vulnerable to attacks. Therefore, the implementation of a secure and integrated key management solution is crucial to support E2EE encryption.

In addition, E2EE encryption can have an impact on system performance. The continuous process of encrypting and decrypting data can slow down the performance of applications and cloud infrastructure. This is especially true for applications with large volumes of data or that require transaction processing in a short period of time (Kalaiprasath et al., 2017). The use of high computing resources for encryption can add to the operational burden and costs incurred by organizations. Besides performance issues, encryption also requires a high level of integration between different systems. For example, if an organization uses various cloud services or third-party applications, all these systems must support and operate with compatible encryption keys. This can be a problem if the cloud service provider or application does not offer full support for the encryption standard desired by the organization. Thus, while E2EE encryption provides excellent protection, challenges related to key management, performance impact, and integration between systems are important factors to consider when planning the deployment of this technology in Cloud Computing.

The Role of Security Policy and Authentication in Strengthening Cloud Security

While end-to-end encryption is a very powerful tool in securing data, data protection in Cloud Computing cannot rely on encryption alone. A clear and comprehensive security policy is an important factor that ensures that encryption can be effectively implemented. Organizations should establish policies that involve role-based access control, good key management, and training for staff responsible for data security

(Paul & Aithal, 2019). The implementation of multifactor authentication (MFA) is also very important to strengthen security. MFA requires users to prove their identity with more than one method, such as a combination of a password and a physical or biometric token. With multifactor authentication in place, organizations can ensure that only authorized users can access sensitive data, even if encryption keys are successfully stolen or predicted by unauthorized parties (Kalaiprasath et al., 2017).

The importance of internal security policies cannot be underestimated either. Employees are often the weak point in an organization's security system, either due to ignorance or unintentional mistakes. Through continuous security training, organizations can raise awareness of the importance of encryption and data protection, and reduce the possibility of data leakage due to human negligence. Role-based access control (RBAC) is one way to ensure that only users who have the right permissions can access certain data. For example, in the financial sector, only employees with authorized access can view sensitive financial information. A strict RBAC implementation will further strengthen encryption defenses by limiting who can access encrypted data. Overall, while end-to-end encryption is an integral part of a cloud security strategy, strong policies in access management and multifactor authentication, as well as awareness and training for staff, will further optimize data protection and ensure that data security in the cloud is truly maintained (Sinha, 2023; Paul & Aithal, 2019).

CONCLUSION

End-to-end encryption is proven effective in improving data security in Cloud Computing. The implementation of encryption can significantly reduce incidents of data leakage, unauthorized access, and cyberattacks, with a reduction in data leakage incidents by 80% and unauthorized access by 83.3%. This shows that encryption can protect sensitive data more effectively, reducing potential losses due to existing threats. However, while encryption can reduce security risks, the biggest challenge lies in the management of encryption keys and their impact on system performance. Improper key management can make it vulnerable to leaks or loss of access, while the performance impact of encryption can potentially disrupt the performance of cloud-based applications that require fast data processing. Overall, end-to-end encryption is an important part of a cloud security strategy, but its success relies heavily on policies that support good key management, integration between systems, and the use of multifactor authentication to protect data from internal and external threats.

REFERENCES

1. Ahmad, M., Pervez, Z., Lee, S., & Kang, B. (2015). Task-oriented access model for secure data sharing over cloud.. https://doi.org/10.1145/2701126.2701186
2. Alemami, Y., Al-Ghonmein, A., Al-Moghrabi, K., & Mohamed, M. (2023). Cloud data security and various cryptographic algorithms. International Journal of Electrical and Computer
3. Eya, N. and Weir, G. (2021). End-user authentication control in cloud-based erp systems., 1-6. https://doi.org/10.1109/nccc49330.2021.9428846
4. Kalaiprasath, R., Elankavi, R., & Udayakumar, R. (2017). Cloud security and compliance - a semantic approach in end to end security. International Journal on Smart Sensing and Intelligent Systems, 10(5), 482-494. https://doi.org/10.21307/ijssis-2017-265
5. Kara, M., Laouid, A., Yagoub, M., Euler, R., Medileh, S., Hammoudeh, M., … & Bounceur, A. (2021). A fully homomorphic encryption based on magic number fragmentation and el-gamal encryption: smart healthcare use case. Expert Systems, 39(5). https://doi.org/10.1111/exsy.12767
6. Lanjekar, A., Thakur, A., Koli, Y., & Katti, J. (2017). Electronic medical reports security in cloud storage environment based on visual cryptography. International Journal of Computer Applications, 179(6), 30-33. https://doi.org/10.5120/ijca2017915969
7. Paul, P. and Aithal, P. (2019). Cloud security: an overview and current trend. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3497705
8. Sinha, S. (2023). Secure cloud storage using end-to-end encryption. International Journal for Research in Applied Science and Engineering Technology, 11(12), 567-574. https://doi.org/10.22214/ijraset.2023.57414
9. Suma, M. and Madhumathy, P. (2022). Brakerski-gentry-vaikuntanathan fully homomorphic encryption cryptography for privacy preserved data access in cloud assisted internet of things services using glow-worm swarm optimization. Transactions on Emerging Telecommunications Technologies, 33(12). https://doi.org/10.1002/ett.4641
10. Yang, P., Gui, X., An, J., & Tian, F. (2017). An efficient secret key homomorphic encryption used in image processing service. Security and Communication Networks, 2017, 1-11. https://doi.org/10.1155/2017/7695751