IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 11, Issue 2 (Mar. – Apr. 2024), PP 10-16
www.iosrjournals.org

The Importance Of Data Encryption Algorithm In Data Security

Tunbosun Oyewale Oladoyinbo
University Of Maryland Global Campus, 3501 University Blvd E Adelphi, Md20783

Oluseun Babatunde Oladoyinbo
Oyo State College Of Agriculture, Igboora, Oyo State.

Adeyemo Isiaka Akinkunmi,
Ladoke Akintola University Of Technology Ogbomos, Oyo State.

Abstract
Data security has become a paramount concern in today's technologically advanced landscape, with data breaches escalating due to sophisticated hacking methods. The importance of data encryption algorithms in preventing unauthorized access without the corresponding decryption key is crucial for individuals and organizations alike. This paper delves into various types of data encryption algorithms, including asymmetric and symmetric encryptions such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Blowfish, and Twofish. These algorithms play a vital role in enhancing data security by safeguarding against threats like ransomware, social engineering attacks, and insider threats. Through a comprehensive literature review and empirical analysis, the significance of data encryption algorithms in data security is explored. The study reveals a positive relationship between investment in data encryption and financial outcomes, emphasizing the importance of robust encryption measures. Further, the study highlights future prospects for data encryption algorithms, including advancements in quantum-safe cryptography and homomorphic encryption. Essentially, data encryption algorithms serve as a crucial component in mitigating data security risks, ensuring data integrity, and compliance with regulations, thus safeguarding individuals and organizations from potential financial and legal ramifications of data breaches.

Date of Submission: 01-04-2024 Date of Acceptance: 10-04-2024

I. Introduction

Data security has emerged as a significant concern in the contemporary landscape, characterized by vast technological advancements to facilitate diverse online operations. Subsequently, the proliferation of data breaches has escalated due to the increasing sophistication of mischievous hackers who devise methods to gain access to confidential information and exploit it for unlawful purposes, such as extortion, blackmail, or larceny (Ali et al., 2021). This is a significant issue for all individuals whose personal information is required by an online program, but especially for those who utilize these applications to make online transactions and are prompted to input their confidential information, like credit card or social security numbers. Likewise, organizations are susceptible to adverse implications due to data security breaches. This is because hackers can illegally access client information, emails, and other vital data, harm a company's reputation, and result in substantial financial losses or lawsuits in extreme encounters (Hammouchi et al., 2019). Since individuals, organizations, and businesses are the primary targets of hackers, it is necessary to explore the underlying importance of data encryption algorithms in data security to prevent unauthorized access without the corresponding decryption key.

II. Literature Review

Noteworthy, it is prudent for anyone or enterprise using a computer or other device capable of storing data or accessing the internet to implement necessary algorithms to encrypt their data. Encrypting data ensures its security by preventing unauthorized access without the corresponding decryption key. Ensuring data security and encryption is critical in managing and maintaining information on data systems. Users' confidence can be significantly enhanced through the implementation of proper data security and encryption algorithms (Aljazaery et al., 2020). Implementing data encryption algorithms within a system aims to identify and combat unauthorized access to critical information. Incorporating security measures and encryption systems makes it feasible to avert data interception, theft, and unauthorized access effectively. Data security further emphasizes the safeguarding of servers and their associated functions. An enormous risk that databases could be exposed to is administrators conducting unauthorized server transactions. Therefore, it is vital to monitor factors like the occurrence of malware outbreaks, overloads, programming and design defects, and physical damage.

Contemporary enterprises must formulate and implement stringent data security measures to ensure compliance with data protection regulations. For instance, it is mandated that institutions or businesses that use and process user payment details enforce robust processes to secure payment data from illegal access. Similarly, health-based organizations in the U.S. are required to safeguard private health information (PHI) in accordance with the stipulations instituted by the Health Insurance Portability and Accountability Act (HIPAA) (Imperva, 2022). As a result, it is arguable that the survival of modern organizations is contingent on data security since it can trigger considerable implications on the client's private data and primary assets in the institution. Moreover, it is essential to note that data incidents and breaches have substantially increased, with over 25,575 user accounts being impacted across the U.S. annually (Imperva, 2022). These occurrences not only contribute to declined trust and reputational damage but can also lead to immense financial losses and legal charges or fines.

In recent years, there has been a noticeable surge in the vigilance with which both organizations and individuals protect their assets and data in response to cybercrime proliferation. This includes organized electronic crime and hostile hacking as hazards. Irrespective of the nature of the information safeguarded, a subset of clientele and customers are invariably interested in the security protocols implemented by the organization and the cloud service providers responsible for maintaining the data and assets (Ali et al., 2021). As a result, fostering transparency regarding the implementation of data encryption algorithms and technologies in a business bolsters client trust and confidence. Through this, customers maintain their loyalty and possibly even recommend the company to others. In essence, the mere emphasis on data encryption has the potential to serve as an exceptionally compelling sales strategy.

Data Encryption Algorithms

Besides, the results of this comprehensive literature review reveal that data encryption algorithms encompass a multitude of diverse approaches to safeguarding databases, entailing asymmetric and symmetric encryptions. Asymmetric encryption integrates the public and private keys, where the former is deployed for data encryption, whereas the latter is highly protected and shared between the sender and receiver to facilitate data decryption (Jacob, 2019). Symmetric encryption relies on a universal key for data encryption and decryption. There are several types of data encryption algorithms that have vast benefits in enhancing data security. These incorporate combinations of public and private key encryptions to protect and hide sensitive data and information from respective users, as well as cipher text retrieval.

Data Encryption Standard (DES)

Primarily, one of the widely adopted types of data encryption algorithms is the Data Encryption Standard (DES). This is one of the most broadly recognized cryptographic systems that are publicly available. Commercial enterprises commonly incorporate DES to offer a standard approach to safeguarding sensitive and classified information (Alhag & Mohamed, 2018). In DES, the encryption and decryption of data are executed using the same key. Ideally, the DES algorithm is comprised of diverse steps, commencing with encryption, use of plaintext block to move bits around, subjecting the key to the key to the Key Permutation to remove the 8 parity bits, and processing of the plaintext and key.

This facilitates splitting the key into two halves, which are rotated based on the round and then recombined and compressed to allow plaintext block encryption. However, it was replaced by Triple DES, an algorithm that was introduced in 1970. This algorithm achieved success subsequent to its inefficacy, owing to the ease with which hackers discovered vulnerabilities to bypass it (Jacob, 2019). Despite the update, the algorithm is still perceived as ineffective since it is susceptible to major attacks when a weak key is employed. Although it is possible to launch an attack against DES in its Triple DES form, this algorithm is preferred due to its reputation for providing a higher level of security.

Advanced Encryption Standard (AES)

In addition, data encryption algorithms include Advanced Encryption Standard (AES). The AES algorithm is attributed to the hasty implementation of software and hardware in fostering data security. It is feasible to incorporate the AES algorithm across diverse platforms since it has been tested and customized to function in numerous data security applications, even in seemingly small technological devices (Smid, 2021). Based on the National Institute of Standards and Technology (NIST) recommendations, the AES has been conceptualized as the ideal and advanced replacement of the DES. This is because the AES algorithm uses key size to determine which 128-bit data blocks to be encrypted in the 10, 12, and 14 rounds (Smid, 2021). To encrypt and improve data security using the AES algorithm, it is necessary to establish the round keys from the cipher key before initializing the state array. In this, the Sub Bytes serve as the encryption site to allow data transformation and interpretation. The transformation proceeds to the new column level before round keys are added to each column in a timely manner to culminate the output.

Rivest-Shamir-Adleman (RSA)

The other notable type of data encryption algorithm with relevant benefits in contemporary data security landscapes is the Rivest-Shamir-Adleman (RSA). Since its development and establishment in 1977, RSA has been integrated as a public key algorithm across vast systems to augment data and information security. This algorithm is conceptualized to facilitate data encryption and guarantee security by allowing access to permitted or concerned users (Sihotang et al., 2020). In developing and implementing the RSA algorithm, there are several steps involved. First, there is key generation prior to the initial encryption of target data. This focuses on creating a private or public key pair, such as two distinctive primes of p and q. Subsequently, these are computed, relative primes are selected, unique integers are computed, and then the private and public keys are returned. The next step embarks on data encryption, where the original plaintext is converted into cipher text (Sihotang et al., 2020). In this, the message is represented as an integer before it is computed. The final process is the decryption, which reverts the encryption process.

Blowfish

Blowfish represents an additional algorithm that was initially devised as a substitute for DES. Every individual message is encrypted in a unique fashion by employing the 64-bit block encryption algorithm of this symmetric tool (Dibas & Sabri, 2021). Due to its resilience, agility, and rapid characteristics, the blowfish algorithm has garnered recognition and success within contemporary industries. An additional benefit is its unrestricted accessibility to the general public, owing to its classification as public domain. Apart from its password management software application, Blowfish is also present on e-commerce platforms that provide secure payment alternatives.

Twofish

Twofish algorithm was designed as the advanced algorithm replacing Blowfish. This employs symmetric encryption, indicating that deciphering 128-bit encrypted data blocks does not necessitate a license (Dibas & Sabri, 2021). Moreover, irrespective of the key's size, the encryption procedure utilized by Twofish uniformly consists of sixteen iterations. This algorithm operates exceptionally quickly in both hardware and software environments, making it one of the swiftest. Consequentially, numerous modern applications that are specifically engineered to encrypt directories and files employ the Twofish algorithm.

Data Security Risks

Relevantly, the research results highlight that data security faces diverse risks due to the vast proliferation of ransomware, social engineering, as well as advanced persistent threats (APTs). Due to the recent technological advances over the past decade, individuals and organizations have found it challenging to defend against these threats (Landoll, 2021). This implies that the prevalence of data security threats can elicit catastrophic damage and harm to the enterprise's data. Private or accidental exposure is one of the most notable data security issues facing small and major organizations in protecting sensitive data. According to Landoll (2021), negligence or unintended exposure of confidential data contributes to more cases of data breaches than malicious attacks across organizations. There are numerous cases of organizational staff sharing, losing, granting access, or mishandling private data due to a lack of comprehension of data security procedures or, typically, due to mistakes. Therefore, it is imperative to ensure that all employees and stakeholders understand the necessary data encryption algorithms to implement to enhance access controls and prevent data loss.

Data security also faces cases of phishing and diverse social engineering attacks. Phishing is a significant data security challenge where attackers and hackers send messages that seem to come from a trusted sender. However, when the recipient opens or clicks the attached contents of the message, they expose their system to malware attacks. Also, these messages are designed to trick the victim into sharing personal and sensitive information by clicking malicious links or attachments (Baillon et al., 2019). Through this, the attackers are provided with a backdoor to compromise the victim's device and system or illegally access an organization's network. In addition, different social engineering attacks are perceived as the primary vectors attackers use to gain access to private and confidential data and information from individuals and corporations. These attacks adopt a similar approach to phishing activities by deceiving the victim into sharing sensitive data or providing the attacker with a backdoor to access private information across different accounts.

Furthermore, data security risks include insider threats, which involve the internal staff inadvertently or intentionally exploiting the enterprise's confidential data. Some of the most common types of insider threats are non-malicious, malicious, and compromised insider threats. With non-malicious insiders, an organization's employee can expose private data due to the lack of knowledge of existing security policies or negligence and accidents. Malicious insiders result when the user is aware of their participation in exposing, stealing, or compromising an institution's confidential data to create adverse harms, exploit the firm, or for personal gains (Zhang, 2018). The compromised insider occurs when an attacker steals and compromises a staff's credentials and accounts without their knowledge. With this access, the attacker proceeds to conduct undetected malicious activities by concealing their activities using legitimate user information. These can create negative implications for the organization due to the challenges in detecting their occurrence across the network and system.

Ransomware also prevails as a significant data security risk with universal implications across organizations. This entails using malware that infects the corporation's devices and systems, allowing the attacker to access data. This implies that the organization's data cannot be used as required without the decryption key. Often, the attacker displays a message or note indicating their requirements or ransom compensation before releasing the key (Muslim et al., 2019). However, this is not always the case, as numerous encounters have led to substantial data losses even after paying the ransom. Since ransomware can quickly spread and infect vast networks and systems, it is imperative to conduct regular backups. Moreover, there are data security risks associated with SQL injection. The advancements in technology have led to this novel technique, where attackers target a specific database and gain access before stealing or carrying out malicious activities. The attackers gain access by injecting malicious code as a query to manipulate the legitimate database (Landoll, 2021). When executed, SQL injection provides the attackers with administrative access to expose the user's data and information in the database, leading to adverse repercussions.

Notably, numerous contemporary corporations are shifting data infrastructure from on-premises to the cloud. This is because the cloud provides a relatively more accessible platform to share and collaborate data across individual and organizational databases. Conversely, it is assertive that this trend of moving to the cloud makes it more complex and challenging to control and prevent data loss. This is based on the consideration that it offers an avenue for illegal access of data from personal devices and networks over unsecured systems. Also, the cloud increases the chances of users unintentionally or maliciously sharing files with private data and information with unauthorized parties (Seth et al., 2022). With this foundational knowledge, it is arguable that there is no simple solution to data security. Regardless, it is essential to consider the efficiencies of data encryption algorithms in combating data protection challenges to improve the corporation's security posture. Hence, it is necessary to formulate and implement creative and robust security measures to augment data security.

Research Questions

1. What are the different types of data encryption algorithms available in data security?
2. What is the importance of data encryption algorithms in data security?
3. What are the outcomes of investing in data encryption algorithms in data security?

III. Methodology

In exploring the importance of data encryption algorithms in data security, this study conducted a study to estimate the association between percentage of revenue a company invests in data encryption and the financial outcomes measured using revenue reported at the end of the year. Data was collected and analysed using excel analysis toolpak.

IV. Results

To verify whether there is a relationship between the two variables, a scatter plot was made and the resulting graph is as depicted in figure 1 below. The graph shows a positive relationship between the two variables.

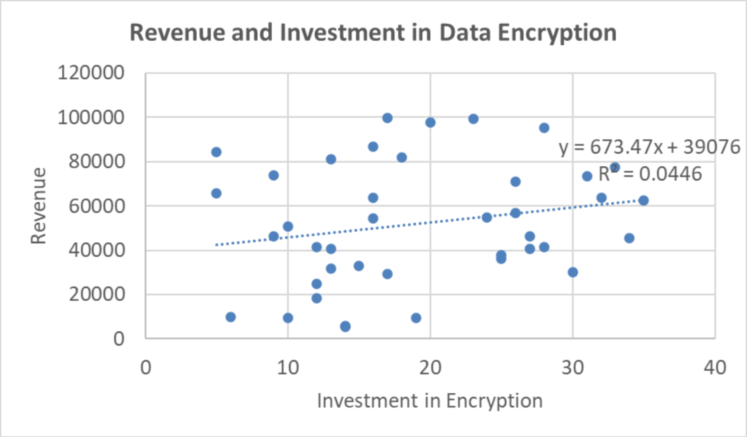
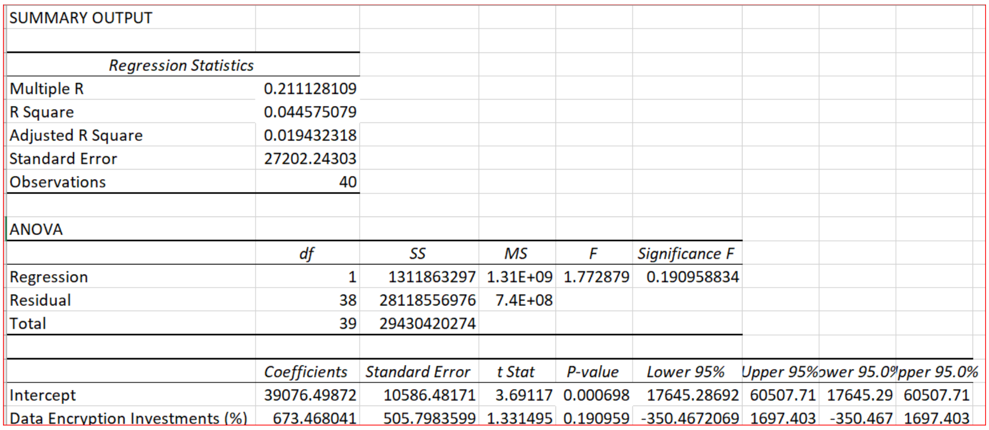


Figure 1: Scatter plot of the two variables

To verify if the relationship is significant, a regression analysis was done. The results of the regression analysis are summarized in table 1 below.



SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.211128109
R Square	0.044575079
Adjusted R Square	0.019432318
Standard Error	27202.24303
Observations	40

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	1311863297	1.31E+09	1.772879	0.190958834
Residual	38	28118556976	7.4E+08		
Total	39	29430420274			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*ower 95.0%*	*pper 95.0%*
Intercept	39076.49872	10586.48171	3.69117	0.000698	17645.28692	60507.71	17645.29	60507.71
Data Encryption Investments (%)	673.468041	505.7983599	1.331495	0.190959	-350.4672069	1697.403	-350.467	1697.403

Table 1: Regression analysis

The coefficient of correlation value of 0.211128109 means that there is a weak linear but positive relationship between the two variables. The coefficient of determination of 0.044575079 means only 4.5% of the variation in the company's revenue can be explained by variation in investment in encryption. This low value of R^2 means that there are other variables behind the level of revenue other than percentage of revenue invested in encryption. The P-value of the model of 0.000698 is less than the level of significance of 0.05 which means that it is significant. As such, the relationship between revenue and percentage invested in encryption is statistically significant.

V. Discussion

In understanding data encryption algorithms in data security, it is fundamental to note that the original data that necessitates encryption is considered as the plaintext or cleartext. To implement data encryption, a sequence of algorithms, which are fundamentally mathematical computations, must be executed on the original data. As highlighted, there are numerous encryption algorithms, each with unique implementation processes optimized for a particular use case and security index. In addition to algorithms, a key for encryption is also necessary. The plaintext is converted to the ciphertext, which represents encrypted data, through the utilization of the key in conjunction with a suitable encryption method (Sajay et al., 2019). Individuals and organizations employ unsecured methods of communication to transmit the ciphertext to the recipient instead of the plaintext. By utilizing a decryption key, the recipient can recover the message to its initial plaintext state once it has reached its intended location. As such, it is critical to ensure the decryption key is kept secure since it may vary from the encryption key.

Essentially, data encryption algorithms are resourceful in data security since they enhance authentication, privacy, regulatory compliance, as well as security. With regard to authentication, utilizing public key encryption makes it possible for individuals and corporations to confirm that the secure sockets layer (SSL) certificate was granted to the appropriate server and that the origin server of the website is the legitimate owner of the private key (Ali et al., 2021). Because there are so many fraudulent websites on the internet, this is an essential feature to have. As an additional benefit, data encryption algorithms prevent anyone other than the intended recipient or the owner of the data from deciphering the messages and gaining access to the stored or shared information. Through the implementation of this protection, critical information is shielded from prying eyes, which may include hackers, Internet service providers (ISPs), spammers, and even government authorities.

It is notable that a great number of industries and government organizations have established policies that mandate the implementation of data encryption algorithms to safeguard user personal data to ensure that they are in compliance with regulatory requirements. As a form of compliance and regulation, data encryption is mandated by laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI-DSS), and the General Data Protection Regulation (GDPR) (McGeveran, 2018). In addition, using data encryption algorithms helps avoid data breaches not only while the data is in transit but also while it is stored. If, for example, sufficient encryption is used, it is likely that the data that is saved on a company device that has been lost or stolen would stay secure. Additionally, parties can engage without the need to worry about data leaks because data encryption algorithms ascertain data safety from potentially destructive and malicious activities like the case of man-in-the-middle attacks.

Data encryption algorithms further facilitate the addition of a second layer of security to individual and corporate data and information. In the context of data security, a significant proportion of security protocols and tools are designed to target malicious hackers and attacks. For example, they possess the ability to detect dubious conduct, detect potential entry points, or thwart unlawful activities. Nevertheless, data encryption algorithms help concentrate on the object that is susceptible to theft (Zhang, 2021). This ensures that in the event that the data is compromised and the security measures intended to prevent assaults prove to be ineffective, sensitive data will not be lost. With robust data encryption algorithms, attackers cannot decipher data since they enable encryption prior to use or transmission. With the additional security layer added by encrypting data, it will take the attacker longer to extract the value from the data, enabling timely detection and mitigation of data security risks. Ultimately, utilizing these algorithms can effectively mitigate the threat of data breach or leakage.

Further, data encryption algorithms are sustainable in augmenting data integrity. This is because data encryption prevents cases of attackers compromising, tampering, or stealing private data and information. It is essential to note that encrypted data is physically unreadable to humans, albeit it does retain critical information such as checksums. This causes data loss, but not theft and decryption failure if modifications are made to encrypted data during the decryption process. By delivering decrypted data, users are assured that it is genuine and untampered. The assimilation of data encryption algorithms also helps prevent adverse financial and legal repercussions resulting from data breaches or losses (Sajay et al., 2019). When data security risks occur, they can lead to fines, lawsuits, and loss of clients, among other negative implications. Consequentially, individuals and organizations must invest in robust data encryption algorithms to encrypt data in store, use, or transit. These algorithms will guarantee that even when third parties access the system or network, they are technically unable to do anything with the accessed data.

VI. The Future Of Data Encryption Algorithms

Inevitably, diverse industries are advocating for the formulation and assimilation of data encryption algorithms on various fronts. In an endeavor to counter brute-force decoding, attempts have been made to increase the size of keys. For instance, numerous additional initiatives are being undertaken to investigate novel cryptography algorithms. An instance of this is a public key algorithm of the next generation that is undergoing quantum-safety testing by the NIST (Alagic et al., 2020). The majority of algorithms that are specifically engineered to operate securely in a quantum environment exhibit limited efficiency when executed on conventional devices. Addressing this necessitates designing accelerators to boost algorithms on x86 platforms in adopted industry operations. As an illustration, homomorphic encryption, a captivating concept, is perceived to enable users to execute computations on encrypted data without the need for pre-existing decryption (Alaya et al., 2020). As a result, respective users can retrieve classified information on an as-needed basis by conducting a database query without the need to consult a superior analyst or request declassification. Homomorphic encryption guarantees data security and protection throughout transmission, usage, and rest. Therefore, using comparable arithmetic as quantum computers elicits additional benefits, making it quantum-safe.

VII. Conclusion

Overall, data security is a critical consideration for all individuals and contemporary organizations. Given that we live in an era characterized by high dependence on technology for different operations, it is imperative to foster data security and information shared or stored across distinct networks, servers, systems, and platforms. As established, there are notable types of data encryption algorithms formulated and implemented to bolster data security. Each approach adopts distinctive processes for encrypting and decrypting data and information. In this context, the common types considered included the DES, AES, RSA, as well as the Blowfish and Twofish. The comprehensive review of pertinent literature reveals some of the significant data security risks facing individuals and corporations. These encompass ransomware, social engineering attacks, as well as advanced persistent threats. These are all tailored to provide the attackers with illegal access to a user's sensitive and confidential data and information. The attackers subsequently compromise and use the data for malicious activities, like causing harm, extortion, requesting ransom, or personal gains. Regardless, data encryption algorithms are vital as they provide an additional layer of data security, streamline authentication, boost client trust and confidence, improve data integrity, and ensure compliance with regulations to prevent financial and legal losses.

References

[1] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Smith-Tone, D. (2020). Status Report On The Second Round Of The Nist Post-Quantum Cryptography Standardization Process. U.S. Department Of Commerce, Nist, 2, 69.

[2] Alaya, B., Laouamer, L., & Msilini, N. (2020). Homomorphic Encryption Systems Statement: Trends And Challenges. Computer Science Review, 36, 100235.

[3] Alhag, N. M. M., & Mohamed, Y. A. (2018, August). An Enhancement Of Data Encryption Standards Algorithm (Des). In 2018 International Conference On Computer, Control, Electrical, And Electronics Engineering (Iccceee) (Pp. 1-6). Ieee.

[4] Ali, B., Gregory, M. A., & Li, S. (2021). Multi-Access Edge Computing Architecture, Data Security, And Privacy: A Review. Ieee Access, 9, 18706-18721.

[5] Aljazaery, I. A., Alrikabi, H. T. S., & Aziz, M. R. (2020). Combination Of Hiding And Encryption For Data Security. Ijim, 14(9), 35. Dibas, H., & Sabri, K. E. (2021, July). A Comprehensive Performance Empirical Study Of The Symmetric Algorithms: Aes, 3des, Blowfish, And Twofish. In 2021 International Conference On Information Technology (Icit) (Pp. 344-349). Ieee.

[6] Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, Simulating Experience, Or Both: A Field Experiment On Phishing Risks. Plos One, 14(12), E0224216.

[7] Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2019). Digging Deeper Into Data Breaches: An Exploratory Data Analysis Of Hacking Breaches Over Time. Procedia Computer Science, 151, 1004-1009.

[8] Jacob, N. M. (2019). Review Of Various Encryption Algorithms. Global Journal Of Computer Science And Technology, 19(E1), 1-3.

[9] Imperva. (2022). What Is Data Security | Threats, Risks & Solutions. Learning Center. Https://Www.Imperva.Com/Learn/Data-Security/Data-Security/

[10] Landoll, D. (2021). The Security Risk Assessment Handbook: A Complete Guide For Performing Security Risk Assessments. Crc Press.

[11] Mcgeveran, W. (2018). The Duty Of Data Security. Minn. L. Rev., 103, 1135.

[12] Muslim, A. K., Dzulkifli, D. Z. M., Nadhim, M. H., & Abdellah, R. H. (2019). A Study Of Ransomware Attacks: Evolution And Prevention. Journal Of Social Transformation And Regional Development, 1(1), 18-25.

[13] Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing The Security Of Cloud Data Using Hybrid Encryption Algorithm. Journal Of Ambient Intelligence And Humanized Computing, 1-10.

[14] Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating Encryption Techniques For Secure Data Storage In The Cloud. Transactions On Emerging Telecommunications Technologies, 33(4), E4108.

[15] Sihotang, H. T., Efendi, S., Zamzami, E. M., & Mawengkang, H. (2020, November). Design And Implementation Of Rivest Shamir Adleman's (Rsa) Cryptography Algorithm In Text File Data Security. In Journal Of Physics: Conference Series (Vol. 1641, No. 1, P. 012042). Iop Publishing.

[16] Smid, M. E. (2021). Development Of The Advanced Encryption Standard. Journal Of Research Of The National Institute Of Standards And Technology, 126.

[17] Zhang, D. (2018, October). Big Data Security And Privacy Protection. In 8th International Conference On Management And Computer Science (Icmcs 2018) (Pp. 275-278). Atlantis Press.

[18] Zhang, Q. (2021). An Overview And Analysis Of Hybrid Encryption: The Combination Of Symmetric Encryption And Asymmetric Encryption. In 2021, 2nd International Conference On Computing And Data Science (Cds) (Pp. 616-622). Ieee.