JKAU: Comp. IT. Sci., **Vol**. **12** No. 1, pp: 27 – 35 (1444 A.H. / 2023 A.D.)
DOI: 10.4197/Comp.12-1.3

Cyber Security Threats and Protection Technologies for Al Rajhi Bank

Abrar Alsayede ،Rania Aboalela
Dept. of Information systems, King Abdulaziz University, Rabigh, Saudi Arabia
aalsayed0169@stu.kau.edu.sa, raboalela@kau.edu.sa

***Abstract*—Technologies are the basis of practically every social action in today's connected world. Although technology has greatly benefited the banking industry, experts have noted the challenges and risks of cybersecurity. A bank can detect, analyze and protect people from these risks thanks to real-time conditions. The majority of financial institutions, including Al Rajhi Bank, are implementing technology in their daily operations as a result of the COVID-19 outbreak [1], which exposes them to cybersecurity issues. The purpose of this project is to investigate and search for encryption algorithms used by Al-Rajhi Bank and what are the most important security attacks that Al-Rajhi Bank faces, as this was done by communicating with an employee in the information technology department at Al-Rajhi Bank, and interviewing. In addition, a literature review of related works, investigation of algorithms and comparison was carried out, in order to verify the efficiency and strength of encryption algorithms in Al-Rajhi Bank and the results of previous works. Al Rajhi Bank's algorithms are very effective and secure, but the various decision-makers believe that as technology develops, financial institutions should think about incorporating other encryption algorithms, like Rivest-Shamir-Adleman (RSA), Triple Data Encryption Standard (TDES), and Twofish algorithms, into their cyber security systems.**

Keywords— Technologies, cybersecurity, Al Rajhi Bank, encryption algorithms, RSA, TDES, Twofish.

I. INTRODUCTION

The majority of firms today operate online, hence a major problem with these businesses is cybersecurity. Numerous studies have been investigated into cybersecurity, including the protection of corporate data and information [2]. Because of the great emphasis that organizations have given to their intricate technological infrastructure, there are now cyber concerns and criminals vying for access to client data and information. Cybersecurity entails taking precautions against illegal disclosure that might jeopardize the accuracy and security of data kept on a network or computer. Cyber security is therefore concentrated on employing technical solutions to protect data, identifying data, and reduce the opportunity of illegal connection. politics have been active in solving cyber interruption, cyberattacks, and cyber thefts. However, there have been enhanced security measures that need be taken in order to address these security problems. Fiscal institutions have expressed concern about the deployment of strategy cyber security technology, regardless of the fact that doing so would be crucial for lowering cyber security risks. This study investigates the algorithms of cyber security defense techniques that are in line with the interests of the organization for Al Rajhi Bank.

II. ALRAJHI BANK: OVERVIEW

Al Rajhi Bank, one of the major fiscal foundations in Saudi Arabia, has been aiming to improve its operations by broadening the selection of services performed to consumers. In line with [3]. In the third period of 2021, the bank's net profit was SAR 10,734 million, and its client base had grown by 44%. It shows that business activities are expanding, which will put financial institutions at risk for cyber security problems [3].

According to Saudi Arabian financial institutions, the integration of advanced technology into the financial industry poses a security concern. Saudi Arabia highlighted the necessity of having rules in place to reduce the risk of cyber threats from hackers by establishing a cyber security campaign with all banking institutions [4]. Financial institutions are at danger from hackers because of the rise in client operations and transactions, which will damage their reputation.

The Saudi Arabian Monetary Authority released the Framework for Cyber Defense in 2017 to protect financial institutions from critical data and ensure that consumer confidence in the financial sector has returned to its highest level.

The continuous process of risk management incorporates the management of cybersecurity, which is essential for attaining operational performance, improving cyber security controls, and recognizing significant flaws in the industry [5]. Having this in place is essential for enhancing the operations' credibility, ensuring that new risks are addressed, and enhancing cyber defense activities. Consideration should be given to Al Rajhi Bank's adoption of cyber security measures, particularly in light of recent cyberattacks and hacking [6].

III. RELATED WORK

Three algorithms—RSA, DES, and AES—have been compared by Seth et al. [7] while taking into account variables like calculation time, memory utilization, and output byte. The main problems with any encryption scheme are these parameters. According to experimental findings, the DES method uses the least amount of memory and the AES algorithm uses the least amount of time for encryption, with just a little difference between the two algorithms' encryption times. The RSA method uses the most memory and takes the longest to encrypt data, while its output bytes are the smallest.

[8] describes a research on cryptography algorithms that examined the security and performance of straightforward encryption methods. Data distribution, pixel count comparison, encryption duration, and encryption quality analyses were carried out when encrypting various picture files. They came to the conclusion that the S-AES and LBlock algorithms offer quick and adequate security while utilizing less resources.

Detailed information on both traditional and contemporary encryption techniques may be found in [9]. The working times of the algorithms and their processor and memory use characteristics were evaluated in the encryptions created using the key employed in contemporary encryption techniques. In this work, just pixels and photos were used.

The correctness, efficiency, and key exchange parameters of a chosen encryption method for BLOWFISH, IDEA, CAST-128, RC6, DES, 3DES, AES, and RSA were examined in [10]. It is stressed that effective encryption systems may be produced by applying to various algorithms.

The performance analyses of the three most popular symmetric encryption algorithms—DES, AES, and Blowfish—were compared in terms of speed, block size, and key size in a study by Thakur et al. Blowfish demonstrated that the encryption technique performs better thanks to the Java simulation tool employed [11].

In [12], the author examined a number of encryption algorithms, including AES, Blowfish, and Twofish, to determine which method offered the maximum security while requiring the least amount of storage space and processing time. They looked at several facets of each algorithm's performance and design. Their results indicated that AES performed better than the other two algorithms.

In order to determine which encryption standard offered the most reliability, dependability, and functionality, Nureni and Sayyidina in [13] examined Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Shamir Adleman (RSA). Both the Java crypto and security packages, which provide a number of security features including authorisation, authentication, decryption, and encryption, were used in the system's implementation. For the study's empirical assessment of these techniques as input files for the encryption process, audio and video files of various sizes were taken into consideration.

As a consequence, it was determined that AES outperformed the other two algorithms in the identical scenario. The algorithms were not employed in this work's mobile health applications, which is a restriction.

In order to evaluate the effectiveness, advantages, and disadvantages of the DES, 3DES, AES, RSA, and Blowfish encryption algorithms, paper [14] examined their performance. They evaluated these algorithms using a number of criteria, including memory, time, and assaults. In terms of memory use, processing speed, and level of security, Blowfish surpassed the competition. The best algorithm in terms of secrecy and integrity was found to be AES.

For various input file contents, lengths, and hardware platforms, Nadeem and Javed [15] compared the performance, including the encryption speed, of the DES, 3DES, AES, and Blowfish algorithms. out of the snort snort snort and sn e's sn't sn't sn't sn't sn't sn't sn't s'. In a number of ways, blowfish outperformed the other three algorithms. While the security of each technique rose with an increase in the number of rounds, the encryption speed fell as the key length and data block length of these algorithms grew.

The performance of several cryptographic algorithms (DES, 3DES, AES, Blowfish, Twofish, Threefish, RC2, RC4, RC5, and RC6) was examined by Nema and Rizvi [16] in terms of throughput, scalability, security, memory use, power consumption, speed, and flexibility. Depending on the factors taken into account and the goal of the encryption, it was discovered that each method had both benefits and drawbacks. The researchers suggested that a user choose the algorithm that is most suited for the application and the user's concerns based on the study's findings. Blowfish is the ideal option if the customer is worried about security, adaptability, memory utilization, and encryption speed.

Bhanot and Hans [17] examined the effectiveness of a number of symmetric and asymmetric cryptographic algorithms to see which one was the best. Based on factors including development, key length, number of rounds required for encryption and decryption, block size, types of attacks discovered, degree of security, and encryption speed, the authors evaluated the advantages and disadvantages of 10 algorithms. It was discovered that the scenario and the parameters used affected each algorithm's strength. For their speed and security, the authors chose Blowfish and ECC as their top choices. Blowfish had not yet been cracked among these methods, although ECC had been.

Wahid et al. [18] examined the performance of the DES, 3DES, AES, RSA, and Blowfish encryption algorithms to assess their performance, strengths, and shortcomings. They evaluated these algorithms using a number of criteria, including memory, time, and assaults. In terms of memory use, processing speed, and level of security, Blowfish surpassed the competition. The best algorithm in terms of secrecy and integrity was found to be AES.

IV. Case Study

A. Research Problem Statement

Al Rajhi Bank is now dealing with cybersecurity attacks that might potentially impair its business operations and reputation. To successfully reduce these risks, the bank must identify the most serious cybersecurity threats and apply the necessary defense solutions.

B. Research Questions

1. What are the most significant cybersecurity threats faced by Al Rajhi Bank?

2. What are the current protection technologies used by Al Rajhi Bank to mitigate these risks?

3. How effective are these protection technologies in mitigating cybersecurity threats?

4. What additional protection technologies can be implemented by Al Rajhi Bank to enhance its cybersecurity posture?.

C. Research Methodology

The goal of this study is to investigate at the encryption methods that Al-Rajhi Bank uses to protect its information technology infrastructure, identify the biggest threats and attacks it faces, and determine the effectiveness of these algorithms via a literary analysis of earlier works. The study strategy will include both primary and secondary data collection techniques.

1) Primary Data Collection: Interviewing an Al-Rajhi Bank employee who works in information technology will be the main technique of gathering data for the threats and encryption algorithms used by Al Rajhi Bank. Depending on

the employee's availability, the interview was either taken place in person or by video conference. The interview questions are designed to elicit details on the encryption methods utilized by the bank.

2) Secondary Data Collection: In order to meet the objective theoretical approach has been used. The theoretical approach is based on review of secondary data acquired from literature survey, books, research papers and articles on the internet.

V. Results And Discussion

A. Threats and Encryption Algorithms In Alrajhi Bank

As a financial institution, Al Rajhi Bank faces numerous cyber security threats that can compromise its customers' data and financial assets. To mitigate these risks, Al Rajhi Bank uses various encryption algorithms to secure its systems and data.

- Phishing attacks: One of the main cyber security risks facing Al Rajhi Bank is phishing attacks. Phishing attacks are dishonest attempts to steal private data like usernames, passwords, and credit card numbers by impersonating a trusted business. These attacks can be started through social media, email, or other channels of contact. Al Rajhi Bank uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption on all connections between its servers and clients to thwart phishing attacks. By encrypting data in transit, the widely used SSL/TLS encryption protocol allows safe communication over the internet.
- Malware assaults: Malware assaults are another danger to Al Rajhi Bank's cyber security. Malware is malicious software intended to harm or interfere with computer systems or to steal personal data. Malware may enter a system through a number of channels, including USB sticks, compromised websites, and email attachments. To prevent malware attacks, Al Rajhi Bank employs a variety of encryption methods, including Blowfish, to thwart malware assaults. A symmetric encryption technique called Blowfish offers robust encryption for sensitive data while it is at rest.

In addition to these measures, Al Rajhi Bank utilizes firewalls and intrusion detection systems to these security measures to monitor network traffic and find any suspicious activities. The bank also does routine penetration tests and security audits to find weaknesses in its systems and fix them before they can be used by attackers.

B. Analysis

On the basis of relevant research by several scholars, a theoretical analysis of the chosen algorithms was conducted. When it comes to communication security, encryption algorithms are crucial. The main issues to consider are battery life, memory usage, and output byte. For performance assessment, the chosen algorithms 3DES, AES, RSA, Twofish, and Blowfish are employed.

Table I makes clear that the algorithms used by Twofish, 3DES, and Blowfish all follow the Fiestel Network, which was created in the early 1970s by cryptography expert Horst Feistel. Substitution, Permutation Network was adopted by AES. The fundamental unit of data that may be encrypted or decrypted in a single operation is the block size. If all other factors are equal, larger Block sizes result in higher security but slower encryption and decryption for a given method. The higher security is attained through more spread. A block size of 64 bits has often been seen as a fair compromise and was used in almost all block cipher designs. Block size used for 3DES and Blowfish is same, 64 bits. However, AES and Twofish both use blocks of 128 bits. A bigger block size is safer. Nevertheless, implementing a big block size is more expensive (in terms of gates or low-level instructions). Another crucial factor in the security of an algorithm is the number of rounds. More rounds provide more security. The Feistel cipher's main characteristic is that it provides insufficient security with just one round. There are sixteen rounds in Blowfish and Twofish. Three times as many rounds as Blowfish and Twofish, 3DES has 48 rounds. Nevertheless, the number of rounds in AES depends on the key length: a key length of 16 bytes has 10 rounds, a key length of 24 bytes has 12 rounds, and a key length of 32 bytes has 14 rounds. Key management is crucial in encryption and decryption techniques. Key search attacks, commonly referred to as brute force attacks, can be used against symmetric key encryption. In these assaults, the attacker attempts every potential key until the message's decryption key is discovered. Before all potential keys are attempted, the majority of assaults are successful. Longer keys reduce the likelihood of successful assaults by expanding the range of potential combination. A variable key length is used by the symmetric algorithms DES, 3DES, AES, and Blowfish. Blowfish performs the best since it has

the longest key length. Moreover, RSA's asymmetric method has changing key lengths. RSA is the best asymmetric algorithm since it has the largest key length.

TABLE I. COMPARATIVE ANALYSIS OF ENCRYPTION ALGORITHMS

Features	3DES	AES	Blowfish	RSA	Twofish
Created By	IBM in 1978	Joan	Bruce Schneier	Ron Rivest 1977	Bruce Schneier
Algorithm Structure	Feistel Network	Vincet	Feistel Network	Asymmetric	Feistel Network
Block size	64 bit	Substitution,	64 bit	variable	128 bits
Rounds	48	Permutation Network	16	Non	16
Key length	112, 168 bits	128 bit	32 bits to 448 bits	1024 to 4096 bits.	128, 192 or 256 bits
Computational Speed	Moderate	10,12,14	Very fast	slow	Fast
Tenability	No	128, 192 or 256	Yes	high	High
Encryption	Low	bits	Very High	slow	High
Decryption Throughput	Low	High	Very High	slow	High
Power Consumption	Highest	Medium	Lowest	low	high
Memory Usage	Very High	Medium	Very low	low	high
Security	Brute force, Chosen plain text, known Plain text	Chosen plain text, known plain text	Dictionary Attack	highest	high
Confidentiality	High	High	Very High	high	Highest
Decryption Throughput	Highest	High	Very High	The highest	High

The length of time it takes an encryption algorithm to convert plain text into encrypted text is known as the encryption time. The throughput of an encryption technique is determined by dividing the total amount of plaintext in encrypted bytes by the encryption time. According to the research, among symmetric methods, Blowfish algorithm takes up the least amount of time for encryption, while 3DES takes up the most time. AES takes longer to encrypt data than DES. Based on encryption throughput, it was determined that Blowfish performed and operated more effectively than 3DES and AES, as well as all other block ciphers. The length of time it takes a decryption algorithm to convert plain text into cipher text is known as the decryption time. The entire amount of ciphertext that has been decrypted in bytes divided by the decryption time is how a decryption scheme's throughput is determined.

According to the analysis, the Blowfish algorithm decrypts data with the least amount of time spent, 3DES decrypts data with the most time spent, and RSA decrypts data with the most time spent. Based on decryption throughput, it was determined that Blowfish outperformed all other block ciphers, including 3DES and AES, in terms of performance and efficiency. Power Consumption is a crucial consideration when choosing encryption algorithms for portable, battery-operated devices. As comparison to DES and AES, 3DES uses more power when it comes to symmetric key algorithms. Yet, compared to DES, 3DES, and AES, Blowfish uses the least amount of electricity. We learned from Blowfish and AES that, when using asymmetric algorithms, Blowfish uses relatively little power—nearly 16% of what AES and RSA do. As comparison to RSA and AES, 3DES uses more RAM when it comes to symmetric key techniques. Compared to Blowfish and 3DES, RSA and AES use less memory. Yet RSA uses the least amount of memory.

Cryptography security determines whether an encryption method is resistant to attacks using plaintext ciphers and brute force. The investigation demonstrates that AES is more secure than 3DES when using symmetric algorithms. Yet, compared to 3DES and AES, Blowfish is thought to be more secure. And the greatest security is provided by RSA and Twofish. It was determined that Blowfish, Twofish, and RSA were capable of provide long-term data security without any backdoor vulnerabilities or key size reduction capabilities. The short key length of DES results in low confidentiality. It has been determined that AES can be employed in situations when great security is required. Blowfish might be utilized in cases involving performance issues. The confidentiality of Blowfish is high as compared to other all mentioned algorithms, and Twofish is the highest.

C. Aditional Enhancement Procedures

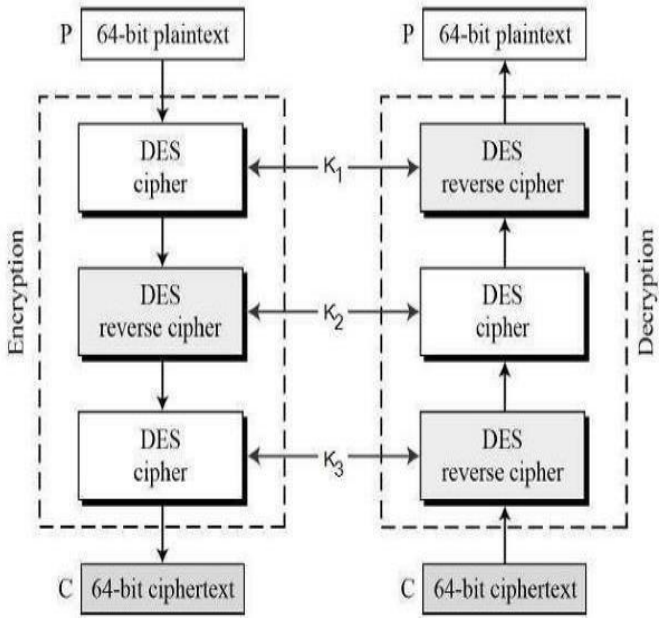

Fig. 1. Encryption-decryption process of Triple DES

Al Rajhi Bank must use powerful encryption algorithms due to the organization's security system's evolving trends. The following are some substitutes advised for the bank:

1) Triple DES: The DES algorithm was created to make it easier to prevent unwanted access to the company's data [19]. The use of three-key encryption came about as a result of hackers rendering the symmetric-key Technology for protecting the organization's data ineffective. The symmetric-key Technology had flaws, which made it less effective in protecting the data from hackers. Plaintext blocks are encrypted using a single DES and K1 key as the initial stage in the encryption process, then the DES reverse cipher using K2. Figure 1 below provides a thorough breakdown of the data encryption-decryption process. This method of system security has been extensively used, and it has proved effective in defending businesses from system vulnerabilities and hacker attacks. The DES algorithm uses a 64- bit key, and the system may support an additional 168 bits in total. Due to its complexity, triple DES is slower and more difficult for hackers to decrypt. As a result, Triple DES encryption may be used for hardware reasons by Al Rajhi Bank, reducing the likelihood that hardware may be compromised by hackers and tightening security measures.

2) RSA: Al Rajhi Bank can also take into account Rivest-Sharmir-Aldeman (RSA) encryption. Because both the private and public keys are readily available, it is regarded as asymmetric encryption. The keys used in the design of the RSA are based on large number techniques in order to secure the system and guarantee that such data cannot be viewed by unauthorized entities. The RSA algorithm is difficult, especially when creating keys since it uses a lot of big integers. As a result, it elevates RSA above DES and enhances the overall security of the material shared inside the company. The improvement of the organization's activities and operations depends on the use of this encryption. By evaluating the financial institutions' data privacy and data reliability, it is possible to enhance the information sharing inside the company.

3) Twofish: Twofish encryption is a popular encryption algorithm used in the financial sector to secure sensitive data. It is a symmetric key block cipher that uses a key size of up to 256 bits, making it one of the most secure encryption algorithms available. Financial institutions use Twofish encryption to protect their customers' personal and financial information, such as credit card numbers, bank account details, and transaction records. This ensures that the data is kept confidential and cannot be accessed by unauthorized individuals. Twofish encryption is also used in electronic payment systems, such as online banking and mobile payments. It provides end-to-end encryption for transactions, ensuring that the data remains secure during transmission.

D. Final Results

- The encryption algorithms used by Al-Rajhi Bank are efficient and sufficient.
- The bank faces various security risks and attacks.
- The most important security risks faced by the bank include phishing, malware, and social engineering attacks.
- The bank uses various security measures to protect against these risks, including firewalls, intrusion detection systems, and anti-virus software.
- The bank also uses encryption to protect sensitive data.
- However, with the advancement of technology, the bank must use other algorithms that keep pace with technological development and progress.
- This is necessary to ensure that the bank's data remains secure in the face of new threats and attacks.
- Additionally, the bank should regularly update its security measures to stay ahead of new threats and attacks.

- This includes conducting regular vulnerability assessments and penetration testing to identify weaknesses in its systems.

Based on the study's findings, Al Rajhi Bank might benefit from using more encryption methods to strengthen its security measures. The study specifically suggested using sophisticated encryption techniques such as TDES and RSA-2048 to provide enhanced safety for sensitive data. A Literature of review were performed to investigate the performance and security capabilities of each algorithm in order to assess the effectiveness of these proposed adjustments.

VI. Conclision

In order to realize the success of the operations and get a competitive edge in the market, it is crucial to employ cyber security measures. Because of the changing nature of the industry, cyber security is now a top concern, and Al Rajhi Bank has to adopt protective measures to better secure the privacy and confidentiality of its customers' data. The Saudi Arabian Monetary Authority has always been vocal about the implementation of the Cyber Security Framework model and has been developing a system for the securitization of the organization's cyber security activities. The basis for developing a safe system for the company should focus on the shifting economic trends and the shifting hacker methods of attack. Using hardware-based Triple DES, RSA, and Twofish encryption can lessen the danger to the bank's database of Al Rajhi Bank. By being more aware of the challenges the company confronts, management may enhance the validity of its movement and the entire security campaign.

A multi-layered approach to encryption is recommended as the best practice for the Saudi banking industry, generalizing the findings of the case study on encryption algorithms for Al Rajhi Bank. This strategy should incorporate key management protocols, symmetric and asymmetric encryption techniques, as well as routine security audits. Also, it is crucial to guarantee that all bank staff members have received cybersecurity best practices training and are aware of the possible hazards related to data breaches. To keep staff members informed of the most recent threats and mitigation techniques, regular security awareness training sessions should be held.

VII. Future work

As a result of the evolving patterns in such measures, there have emerged new trends in measures for cyber security. Therefore, in order to secure the data of such firms, researchers should regularly analyze modifications to cyber security measures and deploy new encryption keys. Future research might also focus on financial institutions in less developed nations to comprehend the difficulties they have while not implementing advanced cyber security measures in their systems.

Also, there are various areas that require further research and study. The use of artificial intelligence (AI) in cybersecurity is another area that needs more research. AI may be used to discover possible dangers before they pose a hazard by detecting abnormalities in network data. Yet, there are also worries that hackers would utilize AI to execute more complex assaults.

Due to time and financial cost constraints, many various modifications, testing, and experiments have been postponed (i.e. The experiments using actual data typically take days or more to complete a single run.). Future development will focus on a more in-depth Create a survey for other banks who have used the three solutions.

References

[1] Z. Omar, “The impact of covid-19 on Islamic banking in Indonesia during the pandemic era,” Journal of Entrepreneurship and Business, vol. 8, no. 2, pp. 19–32, 2020.

[2] A. Loukaka and S. S. M. Rahman, “Discovering new cyber protection Technologies from a security professional prospective,” International journal of Computer Networks & Communications, vol. 9, no. 4, pp. 13–25, 2017.

[3] “Al Rajhi Bank,” Request rejected. [Online]. Available: https://www.alrajhibank.com.sa/en/alrajhi-group/media-center/press-releases/al-rajhi-bank-delivers-sar-10734-million-in- net-profit-for-the-first-nine-months- of-2021. [Accessed: 25-Oct- 2022].

[4] Person, “Online mask ads mystery revealed as Saudi Banks Launch Cybersecurity campaign,” Arab News, 23-Nov-2020. [Online]. Available: https://www.arabnews.com/node/1767466/saudi-arabia. [Accessed: 22-Nov-2022].

[5] M. Abomhara and G. M. Kien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015.

[6] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty security considerations for cloud-supported internet of things,” IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269–284, 2016.

[7] Luo, Z., Shen, K., Hu, R., Yang, Y., & Deng, R. (2022). Optimization of AES-128 Encryption Algorithm for Security Layer in ZigBee Networking of Internet of Things. Computational Intelligence and Neuroscience.

[8] Ü. Çavuşoğlu and H. Al-Sanabani, “The Performance Comparison of Lightweight Encryption Algorithms,” Sak. Univ. J. Comput. Inf. Sci., 2019.

[9] G. F. S. M. Asfiya Shireen Shaikh Mukhtar, “An Introduction of Advanced Encryption Algorithm: A Preview,” Int. J. Sci. Res., 2014.

[10] K. Aggarwal, J. Kaur Saini, and H. K. Verma, “Performance evaluation of RC6, Blowfish, DES, idea, CAST-128 block ciphers,” International Journal of Computer Applications, vol. 68, no. 25, pp. 10–16, 2013.

[11] J. Raigoza and K. Jituri, “Evaluating performance of symmetric encryption algorithms,” 2016 International Conference on Computational Science and Computational Intelligence (CSCI), 2016.

[12] E. Jeevalatha and S. SenthilMurugan, “Evolution of aes, blowfish and twofish encryption algorithm,” International Journal of Scientific and Engineering Research, Vol. 9, No. 4, pp. 115-118, 2018.

[13] A. A. Nureni, A. Sayyidina, “Comparative Analysis of Encryption Algorithms,” Covenant Journal of Informatics & Communication Technology. Vol. 6 No1, 2018.

[14] M. N. A. Wahid, A. K. Ali, B. Esparham, and M. Marwan, “A comparison of cryptographic algorithms: Des, 3des, aes, rsa and blowfish for guessing attacks prevention,” Journal Computer Science Applications and Information Technology, Vol. 3, No. 2, pp. 1-7, 2018.

[15] A. Nadeem and M. Y. Javed, “A performance comparison of data encryption algorithms,” 2005 international Conference on information and communication technologies. IEEE, pp. 84–89, 2005, Pakistan.

[16] P. Nema and M.A.Rizvi, “Critical analysis of various symmetric key cryptographic algorithms,” International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 3, No. 6, pp. 4301-4306, 2015.

[17] R. Bhanot and R. Hans, “A review and comparative analysis of various encryption algorithms,” International Journal of Security and Its Applications, Vol. 9, No. 4, pp. 289-306, 2015.

[18] M. N. A. Wahid, A. K. Ali, B. Esparham, and M. Marwan, “A comparison of cryptographic algorithms: Des, 3des, aes, rsa and blowfish for guessing attacks prevention,” 2018.

[19] R. Ratnadewi, “Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES)..

تهديدات الأمن السيبراني وتقنيات الحماية لمصرف الراجحي

أبرار السيد[١]، رانية أبو العلا[2]

[١، ٢] *قسم نظم المعلومات، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، رابغ، المملكة العربية السعودية*

Aalsayed0169@stu.kau.edu.sa, raboalela@kau.edu.sa

المستخلص. التقنيات هي أساس كل عمل اجتماعي في عالم اليوم المتصل على الرغم من أن التكنولوجيا قد أفادت الصناعة البنكية بشكل كبير، إلا أن الخبراء لاحظوا تحديات ومخاطر الأمن السيبراني. يمكن للبنك اكتشاف وتحليل وحماية الأشخاص من هذه المخاطر بفضل الظروف في الوقت الفعلي. تقوم غالبية المؤسسات المالية بما في ذلك بنك الراجحي بتطبيق التكنولوجيا في عملياتها اليومية خصوصا بعد نتيجة لتفشي [١] COVID-١٩ مما عرضها لقضايا الأمن السيبراني. الغرض من المشروع هو التحقيق والبحث عن خوارزميات التشفير المستخدمة من قبل بنك الراجحي وما هي أهم الهجمات الأمنية التي يواجها بنك الراجحي حيث تم ذلك من خلال التواصل مع موظف في قسم تقنية المعلومات في بنك الراجحي بالإضافة إلى مراجعة الأدبيات للأعمال ذات الصلة والتحقيق في الخوارزميات والمقارنة، وذلك للتحقق من كفاءة وقوة خوارزميات التشفير في بنك الراجحي مع نتائج الأعمال ذات الصلة. تعد خوارزميات بنك الراجحي فعالة وآمنة للغاية، لكن مع تطور التكنولوجيا، يجب على المؤسسات المالية التفكير في دمج خوارزميات التشفير الأخرى، مثل Rivest-Shamir-Adleman | (RSA)، معيار تشفير البيانات الثلاثي (DES وخوارزميات Twofish في أنظمة الأمن السيبراني الخاصة بهم.

الكلمات المفتاحية- التقنيات، الأمن السيبراني، بنك الراجحي، خوارزميات التشفير، RSA، TDES،Twofish.