جامعة الأمير سلطان
PRINCE SULTAN
UNIVERSITY

CYS403 - Security Risk Management, Governance, and Control

Payment Gateway - MADA Pay Alrajhi Bank

مصرف الراجحي
alrajhi bank

Department of Computer & Information Sciences

CYS403 Project deliverable

May 3rd, 2024

Instructor: Dr. Abeer Mirdad

Section: 1267

Students:

Sarah Aljurbua 220410528

Noura Alsaud 220410204

Table of Contents

1. Introduction

With our research paper revolving around the evolving landscape of national finance with the incorporation of security and risk aspects, we were able to choose a payment gateway called MADA Pay, which is known better as a digital payment system used in Saudi Arabia that helps in aiding and facilitating a secure yet convenient electronic transaction of any amount from the comfort of your own phone. To better understand the intricates of the national financial company we chose, we need to better understand MADA Pay and payment gateways in general, MADA Pay is a part of the MADA network which is a national payment scheme set up and operated by SPAN (Saudi Payments Network) that is a subsidiary of the SAMA (Saudi Central Bank). How MADA Pay initiates the payment and wiring of the money is by linking their bank-issued cards (credit or debit cards) to the MADA Pay app. This specialized payment gateway helps promote the 2030 vision by pushing forward the financial inclusion and digitalization of what was once known as a delicate and laborious action (payments of all kinds). In KSA, the landscapes of digitalized and mobilized digital payments have expanded significantly which has offered a variety of payment gateways catering to different needs and preset requirements to its time and date, such as STC Pay, SADAD, Tamara, Tabby, and mostly known Apple Pay. This brings us to the question of why MADA Pay? As previously mentioned, MADA Pay is considered a national backbone of digital payments due to its roots incorporated into SAMA, SPAN, and its pivotal role in the country's financial structure which in turn has helped the widespread and general adaptation of it. However, since our main focus of this research SRM methodology paper is security and risk management, this was the main reason we chose MADA Pay as it has one of the most advanced security features in digitalized payments as well as its known regulatory framework and governance. But talking about MADA Pay's general risks and security is too broad therefore, we have narrowed it down to one company: Alrajhi Bank, as it is one of the largest Islamic commercial banks in the world as mentioned on The Bank Database, 2023 (refer to appendix 1), and that it 'accounts for 42.3% of total global Islamic assets', according to the Saudi Arabia Monetary Authority's annual report (refer to appendix 2). Our main database and data referral in terms of security and risk was "Alrajhi Bank 2023 Annual Report - Unbank the Bank" and all previous annual reports dating back to 2018, as mentioned in our references. We were able to gain the needed insights and references to our SRM methodology through the

400-page extensive annual report findings as well as various media inputs and sites mentioned in the references and appendix section of this paper.

1.1. State-of-the-Art MADA Pay - Alrajhi Bank

When talking about the state-of-the-art overview of Alrajhi Bank's general and MADA Pay's security and risk management, it is essential to emphasize the bank's pioneering role in the financial as well as technical sectors. Given Al Rajhi Bank's stature as one of the leading banks in the Kingdom of Saudi Arabia, its approach to security is both comprehensive and indicative of the latest advancements in financial security technologies due to its renowned commitment to providing secure and innovative banking solutions to the forefront of adopting advanced security measures. Alrajhi Bank's infrastructure is built on robust frameworks that encompass digital encryption, biometric authentication such as face ID recognition, and real-time fraud detection systems which ensure the safeguarding of customers, their transactions, and their data across all of their various banking channels. The bank's efforts to engulf into the sea of MADA Pay and incorporate it into its app and its basic services are emblematic of the bank's efforts to embrace cutting-edge technology while maintaining security and ensuring proper risk management plans are in place. While previous to the incorporation of MADA Pay into Alrajhi Bank's payment gateway options, the risk of fraud and various cyber attacks were prevalent in the other payment gateways which led to the decision to include MADA Pay into Alrajhi's various numbers of payment gateways, as MADA Pay addressed those concerns through advanced - more cyber oriented - security features such as tokenization, E2EE (End-to-End Encryption), 2FA (2 Factor Authentication), SE (Secure Elements), and lastly Dynamic CVV. The introduction of MADA Pay into Alrajhi Bank was back on July 16, 2018, as stated in Arab News, 2018. MADA Pay network was able to introduce e-commerce payments in 2018 as per Mada Pay's informative page (listed in the references), which in turn encouraged Alrajhi Bank to add Visa and prepaid cards as viable MADA Pay cards. In regards to Alrajhi Bank's MADA Pay Advanced SRM features, comprehensive risk assessments were introduced specifically made for MADA Pay as it conducts thorough risk assessments to identify potential security threats which involves analyzing the payment system's vulnerabilities to various types of attacks and cyber frauds such as phishing, malware, and unauthorized accesses.

2. Threat and Risk Assessment

2.1. Listing, Qualifying, and Quantifying Threats

As with every digitalized feature and payment gateway, comes along threats and risks as we continue to progress in implementing it into society and pushing the feature out to the public. In the context of MADA Pay in Alrajhi Bank, multiple different and various types of threats have been identified ranging from socio-economical threats down to natural/ environmental threats and all broad types of threats will be discussed, analyzed, qualified, and then quantified.

Starting the list of threats prevalent in MADA Pay in Alrajhi Bank with the most worrisome: Cybersecurity threats more specifically malwares, phishing, and ransomware attacks targeted at clients/ customers and the bank's workers - ranging from low-level profile workers, all the way to the bank's general branch manager- which all lead to aiming at stealing the user's personal and sensitive information or funds. Such cyber threats faced by Alrajhi Bank are mentioned on the CVE website (mentioned in the references), in relation to cybersecurity threats CVE-201-4197. The estimated financial impact of this threat was calculated to be around 360,000 Saudi Riyals and an extra 120,000 Saudi Riyals to implement rules and regulations to ensure the likelihood of this threat or a similar one is reduced from medium to low. The operational impact of this threat was calculated to be a reduction in Live Status to reach an all-time low of 12%, meaning the apps were down and out of use for safety reasons for about a whole 24 hours, which in turn placed this threat as a high on the risk level assessment. This threat was a risk to the CIA Triad as the confidentiality of the client's information was accessible by unauthorized personnel without a trace. Threat number CVE-2014-419 is a similar threat that caused fraudulent transactions on clients' accounts without their knowledge or their approval. An example of a socio-economic threat faced by Alrajhi's MADA Pay payment gateway not mentioned in CVE was in 2020 during Covid's pandemic strike, as everyone was on lockdown and therefore the usage of the online MADA Pay payment gateway was compromised which made attackers seek possible attacks such as Buffer Overflow attacks on the gateway. This attack was attempted, in August of 2020, and due to its partial failure there were no operational impacts or financial impacts because of the attack itself but there were financial impacts of 375,000 Saudi Riyals due to the implementation of stronger security against those types of attacks, this placed

this specific threat on the low-risk level assessment. This threat is labeled as a partial threat due to the fact that it was able to bypass the system security but was caught before any losses or actual attacks on personal information occurred. Other types of attacks and threats such as political, natural, operational, competitive, and reputational threats were plotted against Alrajhi Bank's MADA Pay payment gateway throughout the years from 2018 to the present year, each with varying financial and operational impacts causing a difference in the risk levels of each, with the most prevalent ones mentioned above.

2.2. Understanding Causes of Threats

In the previous sub-heading, we discussed three prevalent threats of different categories, their operational and financial impact as well as their risk level with other general discussions of general types of threats. In this sub-heading, we will discuss the causes of these threats by understanding them more deeply. (Risk matrix was used). With the first threat, a cyber threat: CVE-201-4197, the most prevalent cause of this threat to have occurred was due to exploited system vulnerabilities in the SQL anti-injection defender via Alrajhi's app, therefore meaning a lack of implemented security measures was a part of the cause as well. This explains why more than 350,000 Saudi Riyals were lost as a financial impact and an extra 120,000 Saudi Riyals to put in place the needed security measures to counter such a threat in the future. The similar CVE threat number 201-419 was due to poor placed security implementation, as many fraudulent transactions of small amounts were able to bypass the system's security, due to having to reimburse every client targeted by this attack the financial impact as well as operational impacts were high placing this threat as a high on risk level via risk level assessment. The second mentioned threat, non-CVE mentionable, was the buffer overflow attempted attack in 2020, this partial attack is solely blamed on a lack of basic system detections and the attacker's ability to exploit the system's vulnerabilities that were mistakenly placed online (without approval or authorization). The other types of threats/attacks faced by MADA Pay payment gateway on Alrajhi were split into two categories: the first being due to the increased digital footprint of Alrajhi Bank, as Alrajhi Bank expanded its features and services such as adding and implementing MADA Pay, more unknown yet and undetected yet vulnerabilities are exploited before the developers are able to discover them and fix them/ place security counters (zero-day attack). The second category falls under human errors, phishing, ransomware, and malware are

mostly human-made errors such as an employee or a client clicking on malicious links, using weak passwords, no 2FA, or giving out personal information to unauthorized impersonators. Any and all approaches to avoiding and mitigating these potential threats are multi-faceted approaches that mainly focus on tech upgrades or personal training, therefore for almost all system security vulnerabilities such as CVE-201-4197, require regular system audits, enhanced detection systems (fraud, attack, and mitigation systems), real-time monitoring, client verification process, zero-day vulnerability protection and regular code security reviews of if integrity is breached, an audit is present. Human error-caused threats and exploits are solved by advanced cybersecurity training about phishing and the need for personal verification from the requestor, as well as continuous sharing and collaboration of all team members to help keep each other involved and informed on any changes or new risks. When it comes to different types of risks, there are always three options: transferring, mitigating, accepting, and avoiding the risk. To categorize the previously listed threats and exploits we need to meet different criteria for each, but to simplify the process if the damage of the threat financially and operationally is low accepting it is the best option considering trying to mitigate or transfer it would cost more financially in comparison to accepting it (only financial cost would be to repair the damages). Mitigating the risk and avoiding the risk require a prior put-in plan for different types of risks that helps put into action plans when needed, therefore this makes it harder for more threats to be mitigated or avoided as the plans can't cover all or most threats (especially the unknown ones yet). The last category is transferring the risk, meaning we try to direct the damages of said threat or exploit to a less important or high-level operation, leading to less financial and operational impacts. Human-error-caused threats are usually put on the accepting and the preplanned plans, unlike all the rest of the mentioned threats in the previous sub-heading that mainly fall under mitigating or transferring if possible. Every company has security policies and guidelines put in place for the customer to ensure that their security implementations obey the needed security standards, and based on these security policies each company can decide how and what is needed to be put into place to ensure more safety and security prior-during-after an attack/ threat. In our case, Alrajhi Bank’s MADA Pay security policies include employee access restriction, anomaly detection to deter SQL injections, and encryptions (DES, 3DES, SSL, AES, RSA, ECC). Other types of security policies places are targeted toward the clients to follow to ensure human error threats are avoided to begin with (refer to references).

2.3. Vulnerabilities, Weaknesses, and Strengths

**Disclaimer: most data regarding vulnerabilities and weaknesses of Alrajhi Bank's MADA Pay are proprietary and require internal assessment.*

In this sub-heading, we will break it down into three categories: Vulnerabilities, Weaknesses, and Strengths. As per the disclaimer above, a lot of Alrajhi's specific and general vulnerabilities in regard to MADA Pay were encrypted or proprietary therefore, the list of vulnerabilities was low. Data breaches are a vulnerability that hasn't been discussed as an exploited threat in 2.1 and 2.2, but the truth is that it has been exploited before even though Alrajhi's security policies ensured that security implementations managed privacy and the CIA triad but some attackers can exploit zero-day attacks or exploit previously patched vulnerabilities related to data leakage or breaches. Third-party vulnerabilities are arising due to the dependence on third-party services to provide payment services (MADA Pay) and this can happen due to inadequate security measures on either end and the lack of discussion of responsibilities for each end. The third and last vulnerability mentioned is API insecurity, as MADA Pay uses 3rd APIs, adequate securities should be in place to ensure that no attacker or exploiter can find a threat he can launch/ exploit.

Next on the agenda is the discussion of weaknesses in Alrajhi Bank MADA Pay, and due to the conflict between trying to provide an easy and seamless process when using the app and its services some weaknesses arise. Weak user authentication can be present in times when UX/UI is placed on a higher pedestal than security and safety, this causes two main issues, the first being the lack of security that now can lead to vulnerabilities being exploited and the other being the lack of promised safety of client's information/assets and the lack of the CIA presence. And just like the changing requirements in this day and age, regulatory compliance and governance changes rapidly making it difficult to regulate requirements across different jurisdictions which potentially leads to compliance gaps that are exploited by attackers. Lastly, going over client-sided weakness. Clients are advised on the needed requirements for a well-protected password, to avoid phishing, and the needed requirements to ensure their security/ safety from their side, the lack of these needed implementations from the clients' side could lead to future vulnerabilities and threats. All these mentioned weaknesses have their own solutions and specific implementations needed, but risk matrix and risk registers need to be put in place to decide on the solution or mitigation plans.

On the bright side of these points, Alrajhi Bank's MADA Pay payment gateway has many notable strengths that were slightly mentioned in previous sub-headings, which mostly revolve around its robust encryption as it uses the top 3 most used and strongest encryption for the FinTech world. Not to mention its new state-of-the-art fraud detection system and its automatic integrity and confidentiality audit/monitor system that both try to ensure it applies to the company's security policies. Lastly, is a combination of customer awareness programs sent over via SMS, E-mails, and even in-app notifications but also the company's ability to have a dedicated Security Research and Development center that investigates and continuously explores the emerging threats and develops countermeasures that apply to the global security standards and regulations as they are also used in their Adaptive Risk Management program.

2.4. Analysis of Current Security Situation

Analyzing Alrajhi Bank's (MADA Pay) current security situation data was taken from Alrajhi's AR 2023 (in references), appears to be stable from a financial perspective, with "Fitch Ratings affirming the bank's Long-Term Issuer Default Rating at 'A-' with a Stable Outlook" (Fitch, 2023) (refer to Fitch Ratings). This suggests that the bank maintains a strong position in terms of financial stability and creditworthiness. (Appendix 4).

However, on the cybersecurity front, Al Rajhi Bank has faced challenges. In December 2023, the bank was targeted by a cyber attack attributed to Anonymous Arabia, a group that has become a significant player in the cyberthreat landscape despite being a newcomer. The attack led to the bank's website going offline. Anonymous Arabia, which operates primarily on the Dark Web, claimed responsibility for this attack, stating it was politically motivated due to Saudi Arabia's oil supply policies (refer to Privacy Affairs reference). In response to cyber threats and to ensure the safety of its operations, Al Rajhi Bank has ongoing security measures in place to protect its digital infrastructure and customer data safety. These measures are critical in safeguarding against the evolving landscape of cyber threats. (Appendix 5).

2.5. National Policies, Compliances and Guidelines

Al Rajhi Bank adheres to several national security standards and guidelines to ensure the security of its customers:

- **Corporate Governance Guidelines:** Al Rajhi Bank must comply with corporate governance guidelines set by SAMA.
- **Information Security Standards**: Al Rajhi Bank must comply with information security standards set by SAMA.
- **Saudi Arabian Monetary Authority (SAMA)**: SAMA is the central bank of Saudi Arabia and regulates banks and financial institutions in the country.
- **Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF)**
- **Sharia Compliance**: As an Islamic bank, Al Rajhi Bank must comply with Sharia principles.
- **Data Protection Regulations** include encryption, secure communication paths, and data privacy.

2.6. Risk Register and Proposed Risk Management Plan

**The risk management plan should be reviewed regularly and updated to adapt to new threats and technological advancements (Last update: 8th of April, 2024).*

2.6.1. Asset Inventory

1- Physical Assets: POS terminals, card readers, cash registers, and ATMs.

2- Intangible Assets: MADA Pay mobile application, payment gateway software, online banking platform, customer transaction data, payment processing data, user authentication data, encryption keys, brand trademarks, software patents, and proprietary algorithms.

3- Financial Assets: Revenue from Mada Pay transactions, cash and national gold reserves, and investments such as stocks and holdings.

2.6.2. Risk Register

Asset Categorization	Asset	Threat	Impact	Likelihood	Risk level	Risk Decision	Risk management
Physical Assets	Card readers	Malfunction or failure	Disruption of payment services	Medium	High	Mitigate	Regular maintenance and backup systems implementation
	Cash registers	Malfunction or failure	Disruption of payment services	Medium	High	Mitigate	Regular maintenance and backup systems implementation
	ATMs	Malfunction or failure	Disruption of cash withdrawal services	Medium	High	Mitigate	Regular maintenance and backup systems implementation
Intangible Assets	Mada Pay mobile application	Software vulnerability	Unauthorized access to customer data	Medium	Medium	Mitigate	Regular software updates and security patches
	Online banking platform	Software vulnerability	Unauthorized access to banking data	Low	High	Mitigate	Encryption of sensitive data and Regular software updates and security patches
	Licensing agreements	Non-compliance	Legal issues and financial penalties	Low	Medium	Mitigate	Compliance monitoring and reporting
Financial Assets	Cash reserves	Loss due to theft or misuse	Financial losses	Low	High	Mitigate	Security measures and controls
	Investments	Financial loss	Decrease in investment value	Low	High	Mitigate	Diversification and risk management strategies

2.6.3. Risk Management Plan According to Risk Register (IS Components)

IS Components (6)	Risk #1	Risk #2	Control #1	Control #2
Hardware	Physical Damage: Natural disasters, accidents, or intentional sabotage.	Hardware Failure: Failure of critical hardware components affecting transaction processing.	Physical Security Measures: Implement access controls, surveillance, and disaster recovery plans to protect against physical threats.	Conduct routine maintenance checks and use redundant systems to mitigate the impact of hardware failure.
Software	Malware and Cyberattacks: Attacks such as ransomware or phishing can compromise system security.	Software Vulnerabilities: Exploitation of software vulnerabilities by attackers.	Regular Updates and Patch Management	Antivirus and Antimalware Solutions
Data	Data Breaches: Unauthorized access to sensitive customer information.	Data Loss: Loss of critical data due to hardware failure or cyberattacks.	Encryption and Access Control: Encrypt sensitive data both at rest and in transit.	Regular Backups

People	Human Error	Insider Threats: Malicious activities by employees or contractors.	Training and Awareness Programs	Monitoring and Incident Response
Procedures	Lack of proper security and operational procedures can lead to vulnerabilities.	Failure to comply with regulations and standards.	Standard Operating Procedures (SOPs): Develop and regularly update SOPs for security and operations.	Conduct regular compliance and security audits to ensure adherence to regulations and standards.
Network	Network Attacks: DDoS attacks, man-in-the-middle attacks, and other network-based attacks.	Unsecured Network Communications: Interception of data transmitted over unsecured networks.	Implement firewalls, intrusion detection systems, and network segmentation.	Secure Communication Protocols: Use VPNs and encrypted communication protocols to secure data in transit.

3. Risk Mitigation

3.1. Development of Mitigation Measures

Cybersecurity Enhancements

- Advanced Persistent Threat (APT) protection systems should be deployed to detect and block more complications usually, those that go unnoticed by traditional security threats.
- Encrypt using the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) all in-transit data within the MADA Pay network and from MADA Pay to outside systems.
- The solution implements tokenization on all the payment details coming from the client: the sensitive data is encrypted into a unique identification symbol hosting all the information but not losing integrity or being secure.

Authentication and Access Control

- The system should also have a technology integration to enable biometric authentication (fingerprint or face recognition) between the customers and employees on secure systems.
- Notify works about PoLP (principle of least privilege) and require only necessary access to complete the tasks.

Security Operations

- Launch a 24/7 center to underlie the SOC to incorporate necessary security warnings and manage the incident response.
- The organization constantly performs red team exercises and penetration tests that challenge the prevailing security controls and places with security weaknesses.

Data Protection and Privacy

- Utilize end-to-end encryption (E2EE) for any data stored and transmitted, using AES-256 algorithms.

- Use techniques such as data masking for all personally identifiable information (PII) displayed in non-secure environments or being used during testing and development.

3.2. Assessment of Residual Risk

- Use various quantitative risk assessment tools to help with calculating possible financial outcomes of the risks that have been mitigated, and adjust the mitigation options based on the outcome of the analysis that has been made with regard to the cost and benefits.
- Examine qualitative evaluations using expert reviews on the leftover risks and consider the responses to adjust the risk management process accordingly.

3.3. Making Risk Decisions

- Established the risk register which would encompass all the risks identified, be they for the purpose of mitigation and those responsible for risk management.
- Write escalation protocols that guarantee that the risks of the highest impact or predicted to be likely will be escalated quickly to senior management's attention for decision-making.

3.4. Implementation of Mitigation Measures

- Develop and provide continuous training on cybersecurity with a regular frequency of training as part of an enterprise-wide cybersecurity awareness program, including phishing simulations and security newsletters.
- Develop an incident response plan (IRP), with a lot more detail in terms of who does what, means of communication, and stages of recovery in case indeed there is a breach or penetration. (Appendix 7)

4. Monitoring

4.1. Enhanced Security Approach

Continuous and Real-Time Monitoring

- Install NIDS and HIDS across MADA Pay's infrastructure for live monitoring of intrusions. The system will block malicious attempts at disrupting operations.
- Security Information and Event Management (SIEM) is a great tool to continuously monitor our systems and find weaknesses by analyzing event records.
- Improve the SIEM with machine-learning processes to progress the system over time.

Threat Intelligence and Vulnerability Management

- Subscribe to leading sources of threat intelligence and use the gathered intelligence to improve the capability for detection of threats.
- Deploy a continuous vulnerability management program with tools such as Qualys or Tenable Nessus, which have the functionality to support periodical scanning and assessment of your IT infrastructure.

4.2. Improvement of CIA Triad

- Provide an automatic data backup and recovery solution that is crypto-based and is held in on-premises and cloud stores, as a way of guarding data availability and cleanliness.
- Implement on quarter-basis business continuity and emergency preparedness drills to detect any bugs inherent in the current procedures and to test the capabilities of the enterprise to remain afloat and restore operations after the crisis event takes place.

5. Conclusion

This conclusion is written to highlight the effectiveness and robustness of MADA Pay's security policies set in place, focusing on its commitment to maintaining high-security standards to aid in protecting users' data and their personal transactions. Those security measures acknowledge the importance of conducting very thorough risk assessments to continuously update security measures. While the system is strong, it emphasizes the need for ongoing vigilance and updates to address the ever-changing landscape of digital payment threats. The conclusion affirms that MADA Pay plays a crucial role in Saudi Arabia's financial ecosystem, supporting the nation's goals for a digitally inclusive economy. The research emphasizes the significance of adaptive risk management strategies in building and maintaining trust among users and stakeholders in MADA Pay.

6. Extras

6.1. Executive Summary

This project involves looking over the entirety of the digital payment system but more specifically MADA Pay, that is currently being managed by SPAN and overseen by the one and only Saudi Central Bank. The main point of this research project is to check the security and risk management of MADA Pay in Alrajhi Bank, which are essential for good security and building customer confidence. This payment system is well-known for its advanced security features, such as biometric authentication, real-time fraud detection, and strict compliance measures. The executive summary highlights the importance of MADA Pay in promoting digital financial inclusion and how it aligns with Saudi Arabia's Vision 2030 to advance its digital economy. It also emphasizes the role of this gateway in providing secure and convenient transaction methods, while also discussing potential risks and strategies to mitigate them in order to maintain system integrity and confidentiality.

6.2. References

- *The Banker's Top Islamic Financial Institutions 2023*. (n.d.). Www.thebanker.com https://www.thebanker.com/The-Banker-s-Top-Islamic-Financial-Institutions-2023-1698828332
- *Al-Rajhi Bank*. (2022, March 23). Wikipedia. https://en.wikipedia.org/wiki/Al-Rajhi_Bank
- *Here is how the GCC's 10 largest Islamic banks rank*. (n.d.). Www.spglobal.com. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/here-is-how-the-gcc-s-10-largest-islamic-banks-rank-57687584
- *About alrajhi bank*. (n.d.). Www.alrajhibank.com.sa. Retrieved April 5, 2024, from https://alrajhibank.com/About-alrajhi-bank
- *Mada Business Card*. (n.d.). Www.alrajhibank.com.sa. Retrieved April 5, 2024, from https://www.alrajhibank.com.sa/en/Business/Cash-Management/Cards/Mada-Business-Card
- *Visa, mada launch "mada Pay" app*. (2018, July 16). Arab News. https://www.arabnews.com/node/1339546/corporate-news
- *mada*. (n.d.). Www.mada.com.sa. https://www.mada.com.sa/en
- *Al Rajhi Bank in 2023*. (n.d.). Www.alrajhibank.com.sa. Retrieved April 5, 2024, from https://www.alrajhibank.com.sa/ir23/index.html
- *Al Rajhi Bank in 2023 | risk management*. (n.d.). Www.alrajhibank.com.sa. Retrieved April 5, 2024, from https://www.alrajhibank.com.sa/ir23/corporate_governance/risk_management.html
- *CVE - Search Results*. (n.d.). Cve.mitre.org. Retrieved April 5, 2024, from https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=alrajhi+bank
- *Al Rajhi Bank in 2022*. (n.d.). Www.alrajhibank.com.sa. Retrieved April 6, 2024, from https://www.alrajhibank.com.sa/ir22/index.html
- *Al Rajhi Bank in 2021*. (n.d.). Www.alrajhibank.com.sa. https://www.alrajhibank.com.sa/ir/index.html

- (No date) *Al Rajhi mada debit card terms & conditions*. Available at: https://www.alrajhibank.com.sa/-/media/Project/AlrajhiPWS/Shared/Home/Personal/Account/Current-Account/PDFs/Debit__Card_Mada__2022_EN.pdf (Accessed: 06 April 2024).
- (No date a) *Almubasher*. Available at: https://www.almubasher.com.sa/retail-mobile/content/Portal%20Content/Legal%20&%20Regulatory%20Requirements/Online%20Security%20Overview/Online_Security_Overview_en_US_Current.pdf?v=20211209_131422358 (Accessed: 06 April 2024).
- *Governance*. (n.d.). Www.alrajhibank.com.sa. Retrieved April 6, 2024, from https://www.alrajhibank.com.sa/en/About-alrajhi-bank/Governance
- *Compliance*. (n.d.). Www.alrajhibank.com.sa. https://www.alrajhibank.com.sa/en/About-alrajhi-bank/Compliance
- (2024). Fitchratings.com. https://www.fitchratings.com/research/banks/fitch-affirms-al-rajhi-banking-investment-corporation-at-a-stable-outlook-10-01-2024
- *Anonymous Arabia Hits the Arabian Bank Al Rajhi*. (2023, December 3). Www.privacyaffairs.com. https://www.privacyaffairs.com/anonymous-arabia-bank-al-rajhi/
- Benabderrahmane, S., Hoang, N., & Valtchev, P. (2024). Hack Me If You Can: Aggregating Autoencoders for Countering Persistent Access Threats within Highly Imbalanced Data. SSRN Electronic Journal. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4781054
- Sireesha, N. (2024). CSKG4APT: A Cyber security Knowledge Graph for Advanced Persistent Threat Organization Attribution. Journal of Interdisciplinary Cycle Research. Retrieved from https://ir.mallareddyecw.com/id/eprint/425/1/17.pdf
- Wang, J., Wang, L., Li, Z., Yu, H., & Shen, X. (2024). Paris: A Practical, Adaptive Trace-Fetching and Real-Time Malicious Behavior Detection System. SSRN Electronic Journal. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4766985

- Li, J., Liu, J., & Zhang, R. (2024). Advanced Persistent Threat Group Correlation Analysis via Attack Behavior Patterns and Rough Sets. Electronics, 13(6). MDPI. Available at: https://www.mdpi.com/2079-9292/13/6/1106
- Qin, Y., Yang, X., Yang, L. X., & Huang, K. (2024). Modeling and Study of Defense Outsourcing Against Advanced Persistent Threat Through Impulsive Differential Game Approach. SSRN Electronic Journal. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4762074

6.3. Appendix

Appendix 1:

Top Islamic financial institutions 2023

Search to sort by country/institution...

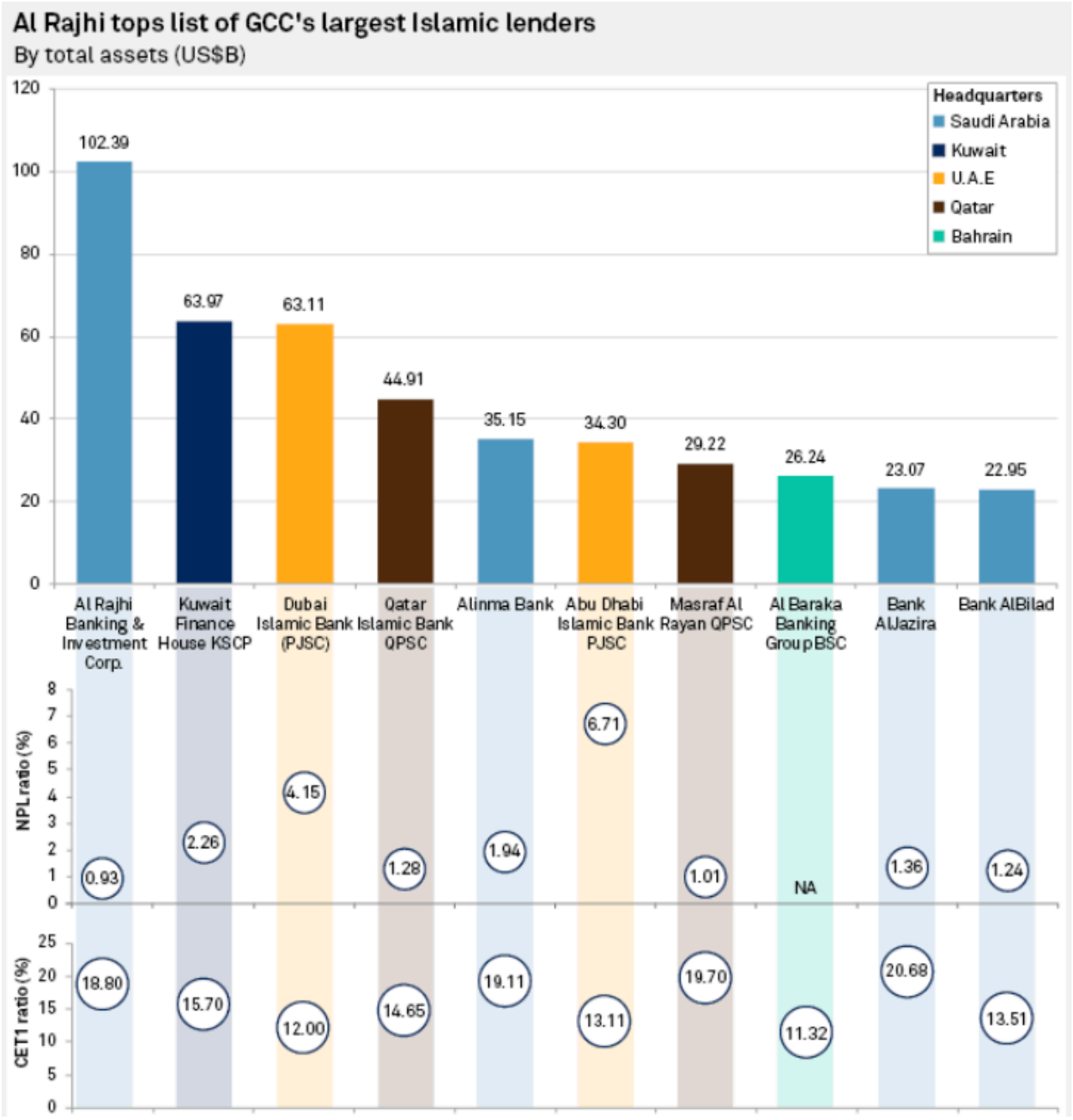
Rank	Institution	Country	Date of results	Sharia-compliant assets ($m)	Chan (%)
1	Al Rajhi Bank	Saudi Arabia	12/22	203,298	22.2
2	Saudi National Bank	Saudi Arabia	12/22	169,702	10.2
3	Kuwait Finance House	Kuwait	12/22	119,256	64.2
4	Dubai Islamic Bank	UAE	12/22	78,475	3.2
5	Maybank	Malaysia	12/22	65,659	4.8
6	Saudi British Bank (SABB)	Saudi Arabia	12/22	55,249	12.5
7	Alinma Bank	Saudi Arabia	12/22	53,450	15.5
8	Qatar Islamic Bank (QIB)	Qatar	12/22	50,550	-5.1
9	Masraf Al Rayan	Qatar	12/22	46,026	-3.7
10	Abu Dhabi Islamic Bank	UAE	12/22	45,880	23.1

1 / 24

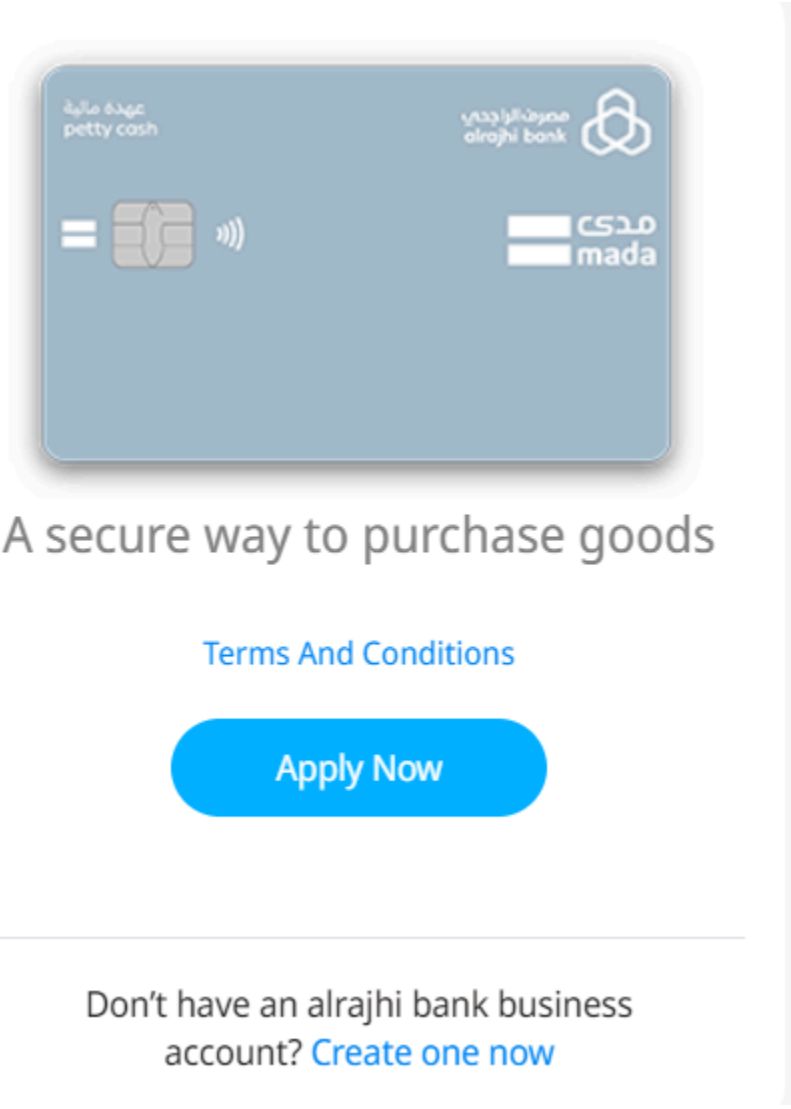
Select each column header to sort

The Banker Database

Appendix 2:


Al Rajhi tops list of GCC's largest Islamic lenders
By total assets (US$B)
Headquarters
Saudi Arabia
Kuwait
U.A.E
Qatar
Bahrain
102.39
63.97
63.11
44.91
35.15
34.30
29.22
26.24
23.07
22.95
Al Rajhi Banking & Investment Corp.
Kuwait Finance House KSCP
Dubai Islamic Bank (PJSC)
Qatar Islamic Bank QPSC
Alinma Bank
Abu Dhabi Islamic Bank PJSC
Masraf Al Rayan QPSC
Al Baraka Banking Group BSC
Bank AlJazira
Bank AlBilad
NPL ratio (%)
0.93
2.26
4.15
1.28
1.94
6.71
1.01
NA
1.36
1.24
CET1 ratio (%)
18.80
15.70
12.00
14.65
19.11
13.11
19.70
11.32
20.68
13.51

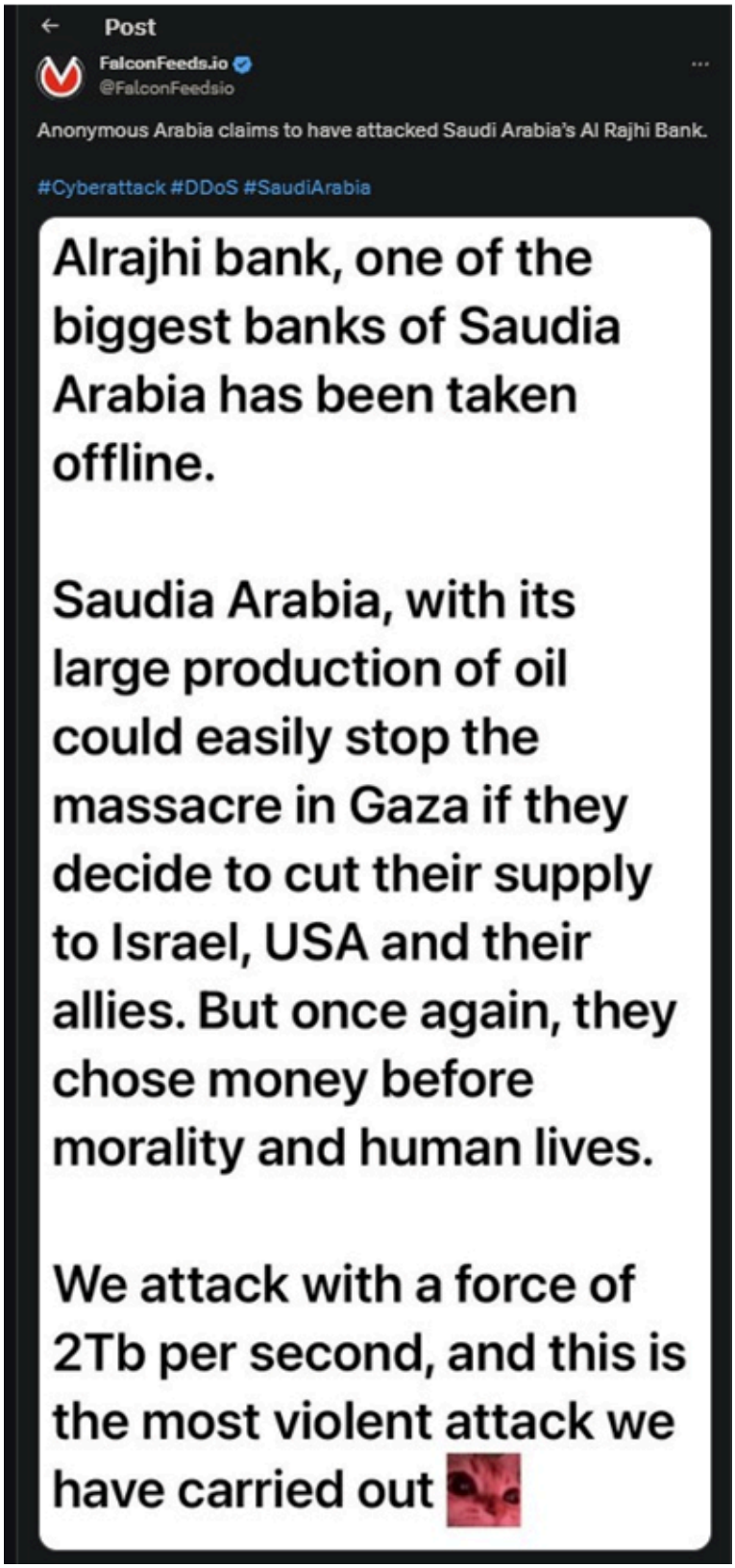
Appendix 3:


عهدة مالية
petty cash
مصرف الراجحي
alrajhi bank
مدى
mada
A secure way to purchase goods
Terms And Conditions
Apply Now
Don't have an alrajhi bank business account? Create one now

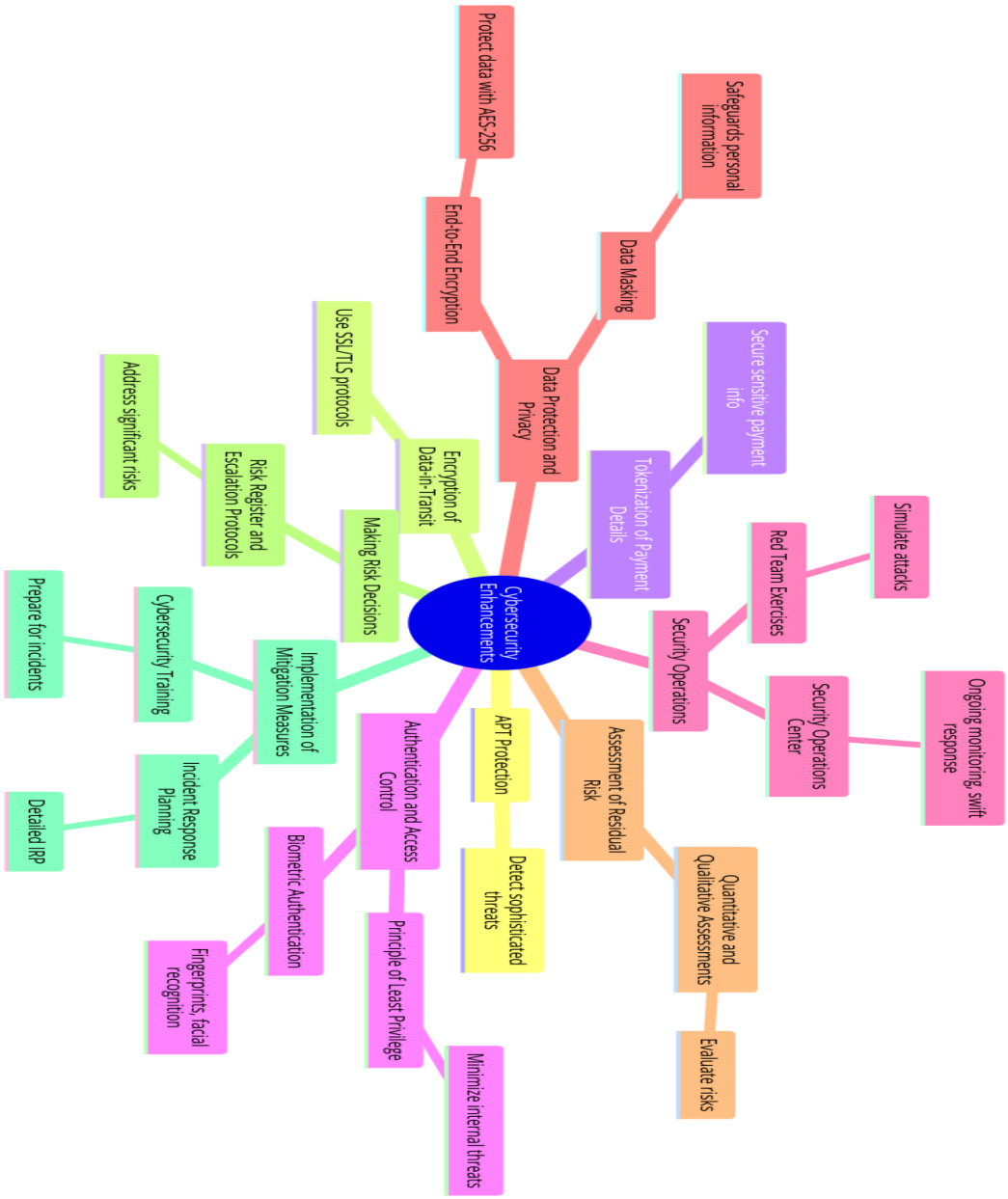
Appendix 4:

ENTITY / DEBT	RATING			PRIOR
Al Rajhi Banking and Investment Corporation	LT IDR	A-	Affirmed	A-
	ST IDR	F2	Affirmed	F2
	LC LT IDR	A-	Affirmed	A-
	Natl LT	AA+(sau)	Affirmed	AA+(sau)
	Viability	a-	Affirmed	a-
	Government Support	a-	Affirmed	a-

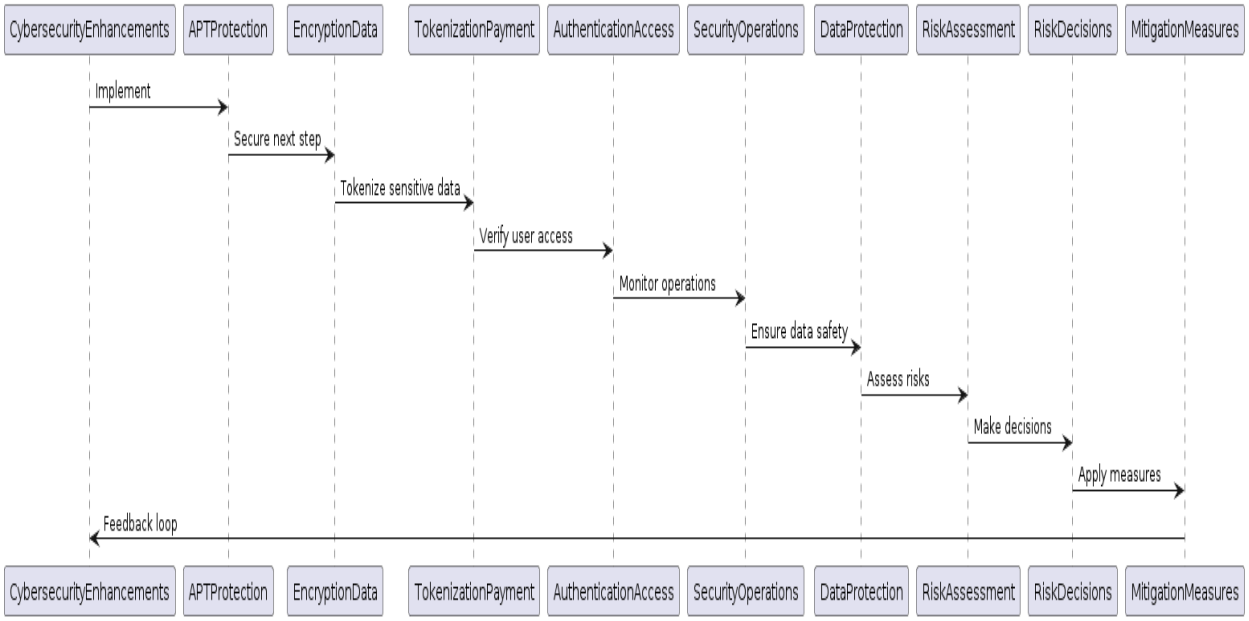
Appendix 5:


Post
FalconFeeds.io
@FalconFeedsio
Anonymous Arabia claims to have attacked Saudi Arabia's Al Rajhi Bank.
#Cyberattack #DDoS #SaudiArabia
Alrajhi bank, one of the biggest banks of Saudia Arabia has been taken offline.
Saudia Arabia, with its large production of oil could easily stop the massacre in Gaza if they decide to cut their supply to Israel, USA and their allies. But once again, they chose money before morality and human lives.
We attack with a force of 2Tb per second, and this is the most violent attack we have carried out

Appendix 6:


Cybersecurity Enhancements
Data Protection and Privacy
End-to-End Encryption
Protect data with AES-256
Data Masking
Safeguards personal information
Tokenization of Payment Details
Secure sensitive payment info
Encryption of Data-in-Transit
Use SSL/TLS protocols
Making Risk Decisions
Risk Register and Escalation Protocols
Address significant risks
Implementation of Mitigation Measures
Cybersecurity Training
Prepare for incidents
Incident Response Planning
Detailed IRP
Authentication and Access Control
Biometric Authentication
Fingerprints, facial recognition
Principle of Least Privilege
Minimize internal threats
APT Protection
Detect sophisticated threats
Assessment of Residual Risk
Quantitative and Qualitative Assessments
Evaluate risks
Security Operations
Red Team Exercises
Simulate attacks
Security Operations Center
Ongoing monitoring, swift response

Appendix 7:



6.3. Work Distribution

Names	Work Distribution
Sarah Aljurbua	#1, #2, #5, #6
Noura Al Saud	#3, #4