Article

Not peer-reviewed version

Top 5 Deadly Cybersecurity Threats to Kingdom of Saudi Arabia

Mariam Alkhalifa , Maha Aljaafari , Saira Muzafar *

Posted Date: 30 August 2024

doi: 10.20944/preprints202408.2244.v1

Keywords: Cyber Crime; Anti-Cybercrime Law; KSA; Ransomware; Dark Web

Article

Top 5 Deadly Cybersecurity Threats to Kingdom of Saudi Arabia

Mariam Alkhalifa, Maha Aljaafari and Saira Muzafar *

College of Computer Science & IT, King Faisal University, Saudi Arabia

* Correspondence: smali@kfu.edu.sa

Abstract: The current era in which we live is centered on information technology because we live in the renaissance of information and its expansion on multiple scales and fields. People who have a high knowledge of technology and a passion for it seek to disseminate this information and process it correctly, and computers have now become one of the most essential devices for government operations. Large companies have already begun to use it in most businesses, and it has helped direct some government procedures for joint e-government, which allows people to access government services from home from their computers. It is also not hidden that with the increase in computer use, electronic crimes increased, and this contributed to the formation of laws. In various countries to deal with them. As technology evolves, the sophistication and impact of these cyber threats continue to grow, posing significant challenges to cybersecurity. This research discusses the role against cybercrime, the regulations, and the allowable behavior of using technology in Saudi Arabia. It analyzes cybercrime in the Kingdom and the system for combating cybercrime.

Keywords : Cyber Crime; Anti-Cybercrime Law; KSA; Ransomware; Dark Web

Introduction

Cyberspace is an intangible and virtual environment that exists in global networks connected by information highways like the Internet. Cyberspace can be used to represent anything like the way people communicate with others and share their knowledge. Users can access this space through computers and global networks [1]. Furthermore, it provides access to vast information and resources, enhancing education and knowledge sharing in many fields. In contrast, people with bad intentions exploit every newest technology to do cybercrime which is any crime that occurs online [2]. Modern cybercrimes result of several reasons like political, cultural, psychological, and economic factors.

Governmental and non-governmental organizations have become more aware of technical information related to most jobs and fields, especially as it contributes to driving innovation and competition among their peers. The recent technology measures are exposed to many risks even the services provided by the government and companies are threaten to several attacks like information leakage, and these risks may lead to their interruption or difficulty in accessing them. Long access to email, affect workflow. Therefore, government organizations must implement a strategy to maintain information security by creating a comprehensive framework that allows their information security program to be developed, formalized, evaluated, and improved to address and address these security risks. Although most organizations have "basic" security measures, the number of security incidents is on the rise [3]. The motive of Saudi Arabia against cybercriminals is to preserve confidentiality by protecting the sensitive information of citizens and the country, availability by ensuring the continuity of services, and integrity by safeguarding against potential disruptions or damage caused by cybercriminals. Making robust cybersecurity measures essential by investing in advanced training and programs. These efforts also align with the country's Vision 2030 initiative, which emphasizes

 doi:10.20944/preprints202408.2244.v1

the importance of a secure and resilient digital infrastructure for sustainable economic growth and development[4].

Background

We can see that Saudi Arabia is one of the nations that take cybersecurity truly: they came the moment in the worldwide positioning of the country's commitment to cybersecurity. It is the nation with 22,5 million cyberattacks per year as well as they had to present various cybersecurity programs, preparation, and instruction assets. They ceaselessly extend their cybersecurity capabilities as well. Yet, a few companies still disregard security and drop casualties to cyberattacks. We have found the best 9 cybersecurity breaches in Saudi Arabia and what we can learn from them.

Cyber Security is an approach that aims to alleviate security concerns and prevent reputational damage, commercial loss, or financial loss. The name "cybersecurity" clearly implies that it is a delicate type of security that we offer to organizations that clients may connect over the internet or a network. There are a variety of handles and ways of sending it. The most important aspect of information defense is that it is a continuous process rather than a one-time solution. To mitigate risk, association owners must keep their assets up to date [5].

Cyber practices in the Kingdom of Saudi Arabia represent a pressing concern in the world. With the advancement in technical sciences, there have been advanced techniques and sites that target them to exploit the weak and try to achieve their goals. Among them, this light appears so far on the important statements, so that we are motivated by protection and sensitive information, and the reality of public freedom is possible the means of the Internet without teenagers. In this, we will learn about what cyber is and its danger to the Kingdom of Saudi Arabia, and we will determine ways to deal with these challenges. Cyber threats contain numerous malevolent exercises that target organizations, systems, and computerized information. They can take numerous diverse shapes, including computer crime, child pornography, cyberbullying, phishing, and selling fakes online. They pose awesome dangers to Web clients, whether they are people or government organizations. This puts the privacy of the data and administrations given at hazard.

This paper is organized as follows: Section 2 presents the KSA strategies to combat cybercrimes, Section 3 discussed the Top 5 cyber threats in KSA. The Cyber-attack impact is discussed in Section 4. The recent case studies are presented in Section 5. And at the end, we have the conclusion in Section 6.

2. KSA Strategy to Combat Cyber Crimes

Here are some methodologies that KSA uses against cyber threats [6]:

1- The Anti-Cyber Crime Law aims at preventing cybercrimes by identifying such crimes and defining their punishments. The objective is to ensure information security, protection of public interest, and morals, protection of rights of the legitimate use of computers and information networks, and protection of the national economy.

2- The National Cybersecurity Authority (NCA) was founded in 2017 under a Royal Order of, King Salman bin Abdulaziz Al Saud. Its purpose is to serve as the primary governing body for cybersecurity in the Kingdom and to act as the central point of contact for all related matters. The primary objective of the NCA is to enhance cybersecurity measures in order to protect the State's crucial interests, national security, essential infrastructures, priority sectors, and government services and operations. Despite the powers and obligations granted to the NCA under its legislation, both public and private companies, as well as any other body, are nonetheless obligated to uphold their cybersecurity responsibilities.

NCA has issued several controls, frameworks, and guidelines related to cybersecurity at the national level to enhance cybersecurity in the country to protect its vital interests, national security, critical infrastructure, and government services. Controls, frameworks, and guidelines issued by NCA include the following: Organizations' Social Media Accounts Cybersecurity Controls, Essential Cybersecurity Controls, Cloud Cybersecurity Controls, Telework Cybersecurity Controls (TCC),

 doi:10.20944/preprints202408.2244.v1

Critical Systems Cybersecurity Controls, Operational Technology Cybersecurity Controls, Data Cybersecurity Controls, The Saudi Cybersecurity Workforce Framework (SCyWF), The National Cryptographic Standards (NCS), The Saudi Cybersecurity Higher Education Framework (SCyber-Edu), Cybersecurity Guidelines for e-Commerce[7]. Figure 1 shows the mission of NCA.

Figure 1. National Cybersecurity Authority (NCA) Mission [7].

3- The National Cybersecurity Strategy was developed to reflect the strategic ambition of the Kingdom in a manner that is balanced between security, trust, and growth. It was created to achieve the concept of (a safe and reliable Saudi cyberspace that enables growth and prosperity) It also includes six main concepts: Integration, Regulation, Assurance, Defense, Cooperation, and Construction. Figure 2 shows the National Cybersecurity Strategy.

Figure 2. National Cybersecurity Strategy[8].

 doi:10.20944/preprints202408.2244.v1

4- The indicative Center for Cybersecurity: To raise awareness of Cybersecurity avoid cyber risks and reduce their effects, the National Cyber Security Guidance Center has been launched to work on issuing alerts about the latest and most serious gaps, and it also works on launching awareness campaigns and programs and cooperates with other guidance centers.

5- **Saudi Federation for Cyber Security:** For the sake of local professional capabilities in Cybersecurity, software development, and drones, the Saudi Federation for Cybersecurity was launched under the Saudi Olympic Committee's umbrella. To provide activities and programs that contribute to increasing community awareness of Cybersecurity, programming, drones, and support and encourage young people to become professionals in this field [9].

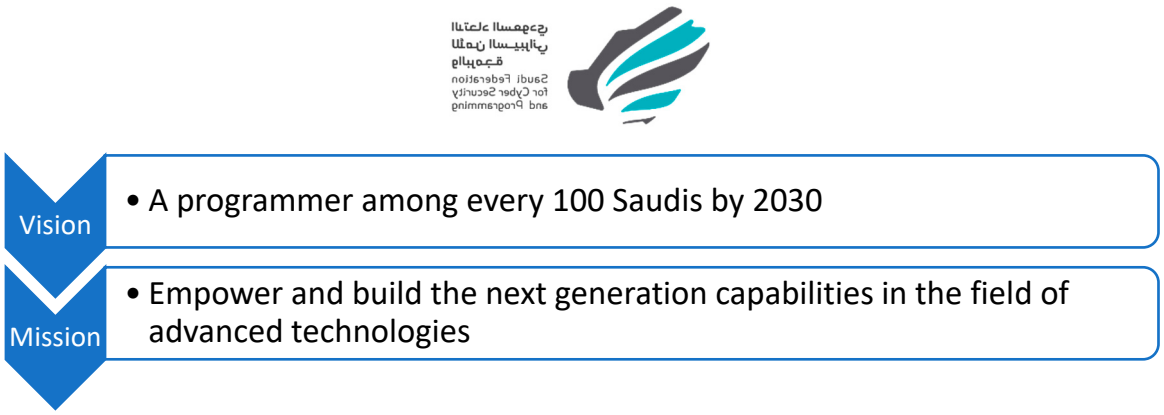

Figure 3. Saudi Federation for Cyber Security Vision and Mission [9].

3. Top 5 Cyber Threats in KSA

What makes Saudi Arabia vulnerable to cyber threats is its global role in producing oil and gas. This is a strong reason for political and economic motivation. These are the top 5 threats in Saudi Arabia based on SOCRadar's and PwC's research. Little more about them: PwC is a community to supports governments and businesses in the region of the Middle East to solve challenges through advisory and consulting. SOCRadar provides an early warning system against cyber threats.

a. Ransomware Threats

One type of malicious software always evolving is ransomware. The attacker encrypts the victim's data making them inaccessible [10]. The reason for the attacker behind this attack is to ask for a ransom then the attacker will make the data available for the victim once again. The attacker might set a time limit for a victim to pay, or the victim might lose his data forever. To make the victim's data available the attacker must provide a decryption key. With all that, it is not guaranteed that all data will not be damaged.

A case happened in 2017 when ransomware called Mamba attacked Saudi corporate networks. By the use of a legitimate tool called DiskCryptor, it encrypts the whole drive disk not just the files. Other adversaries exploited the attacked company to gain access to the company's network. The Mamba ransomware is possibly decrypted by the hacker [10].

The ransomware consists of two phases: The preparation phase and the encryption phase. It first gains access to the organization network and psexec utility (which allows the attacker to run programs in a remote system), the attacker executes the ransomware in the victim's computers and generates a password to lock the DiskCryptor utility. What makes the Mamba ransomware powerful is the inability to restore the encrypted data. DiskCryptor utility uses a very strong encryption algorithm. So, after Mamba encrypted the data they never asked for ransom from the victim, but used it to wipe the data or reveal them to a third party. Saudi Arabia and organizations can use these prevention measures to avoid Mamba ransomware:

- There always should be a backup for important and sensitive information.
- The computers should be protected by strong firewalls and passwords, so no remote entity can access the devices.

 doi:10.20944/preprints202408.2244.v1

- Improve their network to notice suspicious movements, which will limit the spread of ransomware.

b. State-Sponsored Threats

Saudi Arabia is still facing cyberattacks in 2023, according to SOCRadar's research, particularly from APT (advanced persistent threat) [11]. Where a group of intruders acts illegitimate for a permanent time to seek a network to mine up top confidential information. It is presumed that the state-sponsored behind these cyber threats is Iran. The targets of attacks are preplanned and carefully chosen like big organizations or governmental networks. Concernedly outcomes of such threats are:

- Intellectual property is vulnerable to theft (e.g., trade secrets or patents)
- Confidential information is vulnerable to hacking (e.g., employee and user private data)
- Causing damage in critical organizational infrastructures (e.g., database deletion)
- Home page takeovers completely(e.g., filling the page with ads)

Prevention measures Saudi Arabia should follow to protect itself from state-sponsored cyber threats:

Advanced Security Technologies: Invest in cybersecurity technologies, including installing firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection. Also using Multi-Factor Authentication (MFA)

c. Dark Web and Data Breaches

The dark web on the internet is inaccessible through normal browsers. It contains illegal activities where criminals find it easier to steal or sell forbidden things. It allows users anonymity; they don't need to confirm their real identity. Also, whenever users commit a crime on the dark web it is impossible to track them. Secure communication in the dark web also provides privacy for criminals or journalists. The associated illegal activities that users can reach are stolen data, weapons, and drugs. As mentioned, dark web can't be accessed via normal software, Tor or I2P allow users to browse and hide their search history [11].

A case happened to Aramco where a 1 terabyte of data was found in the dark web.[8] The attacker gets access and steals this amount of data from Aramco contains some business information and employees' personal data, such as names, photos, and contact details. The criminals showed just a small part of the data. Then Aramco explained that the released data were not from breaches in their systems. So the leakage of data was probably a leak from third parties [12].

Saudi Arabia and Aramco can strengthen their system by adopting these cybersecurity measures:

- Protect the data from unauthorized access by encrypting the data with a strong algorithm in transit and at rest.
- There should be specialized cybersecurity teams who are trained for fast response whenever a threat happens.

d. Cloud and Connected Devices Vulnerabilities

To cope with future improvement, Saudi Arabia is emerging as the Middle East's largest cybersecurity market, so many organizations tends to use cloud systems [13]. Maybe not all of them have an awareness of security and privacy when using it. Which may result in loss of revenue, customer confidence, and business contraction. A survey was made was conducted in Saudi Arabia [14]. The experts have been asked to prioritize the threats. The result shows that the most dangerous issue is attacks on cloud computing. It can stop users from accessing their accounts by doing to DoS attacks (denial-of-service) threat is sending too many requests to a targeted machine until it can't handle normal operation, which will lead to a loss of system availability. A countermeasure the organization can follow is to apply a filter on request before it is entered into the system [15].

e. Zero-day exploit

Zero-day attacks can cause severe damage by compromising systems before patches are available, posing a serious risk to both public and private sector entities. Unlike known vulnerabilities with available patches, zero-day vulnerabilities lack well-established defenses

 doi:10.20944/preprints202408.2244.v1

that make it possible for attackers to bypass traditional security measures. Another substantial case is the Triton/Trisis attack on a Saudi Arabian petrochemical plant in 2017. The advanced attack was directed at the industrial control systems (ICS) and, by utilizing a zero-day vulnerability, was aimed at influencing the safety systems. The incident could have been far worse, which highlights the aspects of zero-day ransomware, and not just some data but also human lives are at risk [16]. The regular training programs about new methods of zero-day exploitation are beneficial for the organization's cybersecurity field.

Cyber-Attack Impact

Recently Saudi community has faced a high level of risk when new technology appears in the markets. Cyber-attacks are affecting individuals, organizations, and governments [17]. Cybersecurity threats have a significant impact on both individuals and businesses, posing risks to financial stability, data privacy, and operational integrity. Cyber-attacks affect the organization by causing financial and reputation damage, also exposing it to penalty punishments. Data breaches of sensitive data often lead to identity theft and fraud [18]. Malware or ransomware attacks can cause operational disruptions, leading to downtime and reduced productivity. On a larger scale, cyber threats can undermine national security, compromise critical infrastructure, and diminish public trust in digital systems. The increasing complexity of cyber threats requires strong cybersecurity measures to mitigate these risks and safeguard against potential harm. Cybersecurity issues with various application domain [24–28] is becoming increasingly concern for the economies and routine operations. These applications ranges from smart home to smart agriculture [29–32], IoT , smart automations [33–36] to smart logistic industries.

Impact of Cyberattacks on Businesses, Government, and Economy in Saudi Arabia

Cyberattacks can result in substantial financial losses for businesses in Saudi Arabia, disruption of operations due to cyber incidents like ransomware attacks or DDoS attacks can lead to downtime and productivity losses. Financial fraud schemes like phishing scams or Business email compromise (BEC) attacks can result in financial losses for businesses and individuals in Saudi Arabia - Data breaches or cybersecurity incidents can tarnish the reputation of businesses in Saudi Arabia, leading to loss of customer trust and loyalty. Researchers in [17]assess the efficacy of cybersecurity measures at small businesses in Saudi Arabia during a cybersecurity assault, with a specific focus on the consequences of financial harm, loss of sensitive data, and the time required for recovery. Another study highlights the importance of comprehensive cybersecurity measures tailored to small businesses, including technological solutions, policies, and employee education [19,23]. Table 1 shows the top cyber threats to small businesses according to their severity.

Table 1. Top 5 Cyber threats facing small businesses according to their severity[20].

Threat	Description
Phishing and Social Engineering	Phishing involves attackers impersonating trusted sources to trick users into revealing sensitive information or downloading malicious software. It's the most prevalent cyber threat globally, leading to data breaches and financial losses. Measures to combat it include multi-factor authentication (MFA), phishing-resistant authentication tools, and security awareness training.
Ransomware and Malware	Ransomware encrypts company data, demanding payment to decrypt it, causing significant financial damage. It's increasingly sophisticated, with attackers now employing double extortion tactics. Prevention strategies include zero trust architecture, endpoint protection, data backup, and recovery solutions.

 doi:10.20944/preprints202408.2244.v1

Weak Passwords	Weak passwords weaken cybersecurity defenses, making it easier for attackers to compromise accounts. Practices such as password managers, strong password policies, and multi-factor authentication (MFA) mitigate this risk. Emerging solutions like FIDO2 Passkeys aim to replace passwords entirely for enhanced security.
Poor Patch Management	Outdated software and systems are vulnerable to cyber-attacks exploiting known vulnerabilities. Effective patch management tools and strategies ensure timely updates across all devices and networks, reducing exposure to threats like malware and ransomware.
Insider Threats	Insider threats arise from employees or associates with access to critical data, posing risks through malicious actions or inadvertent mistakes. Mitigating insider threats involves implementing strict access controls, monitoring systems, and ongoing employee training on data security practices.

Government agencies in Saudi Arabia may incur substantial financial costs in responding to cyber incidents, including investigation, remediation, and recovery efforts. Persistent cybersecurity threats may undermine investor confidence in Saudi Arabia. Cybersecurity breaches affecting government systems can erode public trust and confidence in the government's ability to safeguard sensitive information. Additionally, intellectual property theft resulting from cyberattacks can stifle innovation and technological advancement in key sectors of the Saudi economy. To mitigate cybersecurity risks, businesses and government entities may need to invest in compliance measures, such as cybersecurity training, infrastructure upgrades, and regulatory compliance initiatives, leading to increased operational costs.

Besides that, the dark web has legitimated uses for privacy and free speech, its anonymity and lack of regulation make it a haven for criminal activities. Cybercriminals exploit the dark web to launch attacks, exchange hacking tools, and coordinate cyber operations, further exacerbating the threat landscape. The challenges in policing the dark web underscore the importance of putting international united agreements cybersecurity strategies to combat illicit activities. For Saudi Arabia's economic stability and the trust of citizens and investors, investing in preventive cybersecurity measures and fostering a cyber-aware culture, Saudi Arabia can mitigate the financial risks and continue its evolution in the digital world.

5. Cyber Espionage and Ransomware Attacks in KSA

In this section we present two most recent cyber-attacks happened in Saudi Arabia.

Case Study 1: Hackers Hit Virgin Mobile in Saudi Arabia.

In 2020, Hackers gained access to Virgin Mobile's office network in Saudi Arabia by exploiting a Microsoft Exchange vulnerability. This incident resulted in the compromising of the company's email system and an Active Directory domain controller. Following a compromise, Virgin Mobile KSA secured its network and implemented measures to prevent further unwanted access. The organization reported that no consumer data was exposed, but only internal emails, reports, and spreadsheets were taken. Virgin Mobile KSA had a breach but did not reveal how it occurred. The corporation is focused on cybersecurity and has instructed staff to protect their personal and professional information[21].

Case Study 2: Records of Healthcare Benefits Management Firm GlobeMed Saudi Got Compromised.

GlobeMed Saudi, a healthcare benefits management organization, had a data breach in 2021, during which hackers gained access to their network and stole critical information. It is suspected

 doi:10.20944/preprints202408.2244.v1

that the hackers exploited compromised credentials to access a distant program. The program's absence of multifactor authentication may have contributed to the hack. A data breach occurred at GlobeMed Saudi, a healthcare benefits management organization, in 2021. Hackers entered the network and stole important data. It is suspected that compromised credentials were utilized to gain access to an application via remote network access. The incident may have been avoided with multifactor authentication. Hackers broke into GlobeMed Saudi's network and moved freely, indicating they had ample time to grab a large amount of data. The corporation has not acknowledged the entire scope of the stolen material, but the hackers have begun to distribute it. The incident highlights the critical importance of cybersecurity in healthcare and the need for stronger safeguards to protect sensitive data. To prevent unwanted network access, organizations should use robust security protocols such as multifactor authentication. Saudi Arabia has made major efforts in cybersecurity, training, and education. The Saudi Monetary Authority has enacted legislation to guarantee that financial institutions have effective cybersecurity safeguards. The National Cybersecurity Authority was formed to manage cybersecurity operations and protect key infrastructure [22].

6. Conclusion:

In summary, technology is important for the operation of individuals, businesses, and governmental organizations. As technology rises and integrates into various sectors, the dangers associated with cybercrime have significantly increased. Saudi Arabia has identified this challenge and has taken substantial steps to prevent cyber threats through vast legislation and robust cybersecurity frameworks. Saudi's Anti-Cyber Crime Law and the initiatives by the National Cybersecurity Authority (NCA) showcase the measures being implemented to protect vital interests, national security, and essential infrastructure. Despite these actions, Saudi Arabia remains vulnerable to cyber threats due to its powerful global role in the oil and gas sector, making it a target for malicious activities. Highlighting the need for continued enhancement of cybersecurity strategies. The effects of cyber threats spread beyond economic losses, impacting national security, citizen trust, and operational integrity. Thus, a wide approach involving advanced security technologies, training programs, and international collaboration is essential to mitigate these risks.

References

1. F. Momeni, "The impact of social, cultural, and individual factors on cybercrime," *Educ. Adm. Theory Pract.*, vol. 30, no. 5, pp. 10152–10159, May 2024, doi: 10.53555/KUEY.V30I5.4716.
2. "View of A review of cyber crime." https://dzarc.com/social/article/view/244/230 (accessed Jul. 25, 2024).
3. S. Muzafar and N. Z. Jhanjhi, "Success Stories of ICT Implementation in Saudi Arabia," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-1851-9.ch008*, pp. 151–163, Jan. 1AD, doi: 10.4018/978-1-7998-1851-9.CH008.
4. "Exploratory Study to Measure Awareness of Cybercrime in Saudi Arabia | Request PDF." https://www.researchgate.net/publication/359330097_Exploratory_Study_to_Measure_Awareness_of_Cybercrime_in_Saudi_Arabia (accessed Jul. 25, 2024).
5. S. K. Ratangiri, "Research Paper on Cyber," no. June, 2021.
6. "Unified National Platform GOV.SA." https://www.my.gov.sa/wps/portal/snp/content/cybersecurity/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zijQx93d0NDYz8DczCLA0CQ4KCg1zMfL2CQ8z1g1Pz9AuyHRUBbL0PTQ!!/ (accessed Jul. 24, 2024).
7. "National Cybersecurity Authority." https://nca.gov.sa/en/ (accessed Jul. 27, 2024).
8. "The National Cybersecurity Strategy." https://nca.gov.sa/en/national-cybersecurity-strategy/ (accessed Jul. 27, 2024).
9. "الاتحاد السعودي للامن السيبراني والبرمجة والدرونز." https://safcsp.org.sa/en/about-us (accessed Jul. 27, 2024).
10. R. A. Al-Mulhim, A. Al-Zamil, F. M. Al-Dossary, and S. Arabia, "Cyber-attacks on Saudi Arabia Environment," *Int. J. Comput. Networks Commun. Secur.*, vol. 8, no. 3, pp. 26–31, 2020, Accessed: Jul. 25, 2024. [Online]. Available: www.ijcncs.org
11. "Saudi Arabia (Ksa) Threat Landscape Report," 2023, [Online]. Available: www.socradar.io

12. "Stolen Saudi Aramco Data Offered on the Dark Web." https://jpt.spe.org/stolen-saudi-aramco-data-offered-on-the-darkweb (accessed Jul. 26, 2024).
13. "Digital Trust Insights 2024 - The KSA perspective." https://www.pwc.com/m1/en/publications/middle-east-digital-trust-insights-2024/the-ksa-perspective.html (accessed Jul. 26, 2024).
14. R. Al Nafea and M. Amin Almaiah, "Cyber Security Threats in Cloud: Literature Review," *2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc.*, pp. 779–786, Jul. 2021, doi: 10.1109/ICIT52682.2021.9491638.
15. J. S. A. Koshy, S. W. Ping, C. Y. Hui, T. Q. Hui, and S. Muzafar, "From On-Premises to Cloud: Crafting Your Pathway for Migration Success," Nov. 2023, doi: 10.20944/PREPRINTS202311.0841.V1.
16. О. С. Саприкін, "Моделі і методи діагностування Zero-Day загроз в кіберпросторі," *Вісник сучасних інформаційних технологій*, vol. 4, no. 2, pp. 155–167, Mar. 2021, doi: 10.15276/HAIT.02.2021.5.
17. F. Alharbi *et al.*, "The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia," *Sensors 2021, Vol. 21, Page 6901*, vol. 21, no. 20, p. 6901, Oct. 2021, doi: 10.3390/S21206901.
18. S. Muzafar, M. Humayun, and S. J. Hussain, "Emerging Cybersecurity Threats in the Eye of E-Governance in the Current Era," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-9624-1.ch003*, pp. 43–60, Jan. 1AD, doi: 10.4018/978-1-7998-9624-1.CH003.
19. A. M. AlBar and M. R. Hoque, "Factors affecting the adoption of information and communication technology in small and medium enterprises: a perspective from rural Saudi Arabia," *Inf. Technol. Dev.*, vol. 25, no. 4, pp. 715–738, Oct. 2019, doi: 10.1080/02681102.2017.1390437.
20. "The Top 5 Biggest Cybersecurity Threats That Small Businesses Face And How To Stop Them | Expert Insights." https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/ (accessed Jul. 30, 2024).
21. "Exclusive: Hackers Hit Virgin Mobile in Saudi Arabia." https://www.bankinfosecurity.com/hackers-hit-virgin-mobile-in-saudi-arabia-a-15018 (accessed Jul. 27, 2024).
22. "Healthcare entities in Saudi Arabia, Illinois, and Mississippi fall prey to Xing Team – DataBreaches.Net." https://databreaches.net/2021/06/11/healthcare-entities-in-saudi-arabia-illinois-and-mississippi-fall-prey-to-xing-team/ (accessed Jul. 27, 2024).
23. Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In *2018 4th International conference on computer and information sciences (ICCOINS)* (pp. 1-5). IEEE.
24. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A review of intrusion detection system using machine learning approach. International Journal of Engineering Research and Technology, 12(1), 8-15.
25. Ray, S. K., Pawlikowski, K., & Sirisena, H. (2009). A fast MAC-layer handover for an IEEE 802.16 e-based WMAN. In AccessNets: Third International Conference on Access Networks, AccessNets 2008, Las Vegas, NV, USA, October 15-17, 2008. Revised Papers 3 (pp. 102-117). Springer Berlin Heidelberg.
26. Gouda, W., Almurafeh, M., Humayun, M., & Jhanjhi, N. Z. (2022, February). Detection of COVID-19 based on chest X-rays using deep learning. In Healthcare (Vol. 10, No. 2, p. 343). MDPI.
27. Humayun, M., Sujatha, R., Almuayqil, S. N., & Jhanjhi, N. Z. (2022, June). A transfer learning approach with a convolutional neural network for the classification of lung carcinoma. In Healthcare (Vol. 10, No. 6, p. 1058). MDPI.
28. Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi, N. A. Malik and M. Humayun, "Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257607.
29. Lim, M., Abdullah, A., Jhanjhi, N. Z., Khan, M. K., & Supramaniam, M. (2019). Link prediction in time-evolving criminal network with deep reinforcement learning technique. IEEE Access, 7, 184797-184807.
30. Ramanjot, Mittal, U., Wadhawan, A., Singla, J., Jhanjhi, N. Z., Ghoniem, R. M., ... & Abdelmaboud, A. (2023). Plant disease detection and classification: A systematic literature review. Sensors, 23(10), 4769.
31. Khairandish, M. O., Sharma, M., Jain, V., Chatterjee, J. M., & Jhanjhi, N. Z. (2022). A hybrid CNN-SVM threshold segmentation approach for tumor detection and classification of MRI brain images. IRBM, 43 (4), 290–299.
32. Dash, S., & Verma, S. (2022). Kavita; Jhanjhi, NZ; Masud, M. Baz, M. Curvelet Transform Based on Edge Preserving Filter for Retinal Blood Vessel Segmentation. Comput. Mater. Contin, 71, 2459-2476.

 doi:10.20944/preprints202408.2244.v1

33. Khan, A., Jhanjhi, N. Z., Hamid, D. H., & Omar, H. A. (2024). Internet of Things (IoT) Impact on Inventory Management: A Review. In N. Jhanjhi & I. Shah (Eds.), Cybersecurity Measures for Logistics Industry Framework (pp. 224-247). IGI Global. https://doi.org/10.4018/978-1-6684-7625-3.ch008
34. Midha, S., Verma, S., Mittal, M., Jhanjhi, N. Z., Masud, M., & AlZain, M. A. (2023). A Secure Multi-factor Authentication Protocol for Healthcare Services Using Cloud-based SDN. Computers, Materials & Continua, 74(2).
35. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., & Gaur, L. (2024). Securing the digital supply chain cyber threats and vulnerabilities. In Cybersecurity Measures for Logistics Industry Framework (pp. 156-223). IGI Global.