A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia

Ahmad Alshammari
Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Saudi Arabia
ahmad.almkhaidsh@nbu.edu.sa (corresponding author)

Received: 5 June 2023 | Revised: 20 June 2023 | Accepted: 26 June 2023

 DOI: https://doi.org/10.48084/etasr.6091

ABSTRACT

Many organizations around the world suffer large losses due to unexpected risks which can have a profound impact on their survival. This paper presents a novel security framework to address the security needs of Saudi organizations. There are four stages in the security framework: risk assessment and management, security intelligence and analytics, security policies and procedures, and security monitoring. A comprehensive security solution was provided by combining common security frameworks, e.g. ISO/IEC 27001:2013, NIST Cybersecurity Framework, and COBIT. The developed framework was designed to help Saudi organizations identify, assess, and control risks and respond to unexpected events in a timely and effective manner. It is expected to help organizations develop and implement effective security measures to protect their critical assets and operations from security threats. The proposed framework is comprehensive and can cover most organizations' requirements.

Keywords-security frameworks; security models; ISO/IEC 27001:2013; NIST cybersecurity framework; COBIT

I. INTRODUCTION

Many organizations experience a global revolution in governance that could affect how they manage their information. Organizations must ensure that their information is adequately protected and in compliance with information security laws [1]. A company's chief information officer should not only be responsible for securing data but also handle them as part of its governance practices. It is critical to note that corporate information security governance includes accountability to shareholders, compliance with legal requirements, setting well-planned security policies, spearheading security awareness and education, defining roles and responsibilities within an organization, establishing contingency plans, and implementing best practices [2]. The security of Saudi Arabian organizations is becoming increasingly important. The current challenges include a lack of emergency response plans that can lead to confusion and chaos during a crisis, poor risk management practices that can cause a company to be unprepared for a potential disaster, inadequate investment in cyber security infrastructure that can leave organizations vulnerable to cyberattacks, weak internal control systems that can leave organizations open to fraud and corruption, poor data protection and backup measures that can cause a company to lose important data in the event of a disaster, poor communication and collaboration between departments that can lead to delays in responding to an incident or event, insufficient training and awareness on emergency response procedures that can lead to mismanagement and errors, and inadequate insurance coverage that can leave a company exposed to financial losses due to an incident or event.

This study aims to develop a novel security framework using the Design Science Method (DSM) for Saudi organizations to avoid or mitigate expected incidents and risks. The proposed security framework embeds four stages, derived from existing security frameworks, such as ISO/IEC 27001:2013, NIST Cybersecurity Framework, and COBIT: risk assessment and management, security intelligence, security policies, and security monitoring. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continuously improving Information Security Management Systems (ISMS) [3]. The NIST Cybersecurity Framework embeds 5 steps and translates the meaning of documents, such as ISO/IEC27001, into understandable information [4]. COBIT is an internal control structure of policies, procedures, and practices to provide organizational results and prevent, detect, and improve undesirable actions [5]. The proposed framework could enable Saudi organizations to better protect their data and systems and manage their security posture.

II. RELATED WORKS

Many studies addressed the security concerns of Saudi Arabian organizations and companies. In [6], various

cyberattacks in Saudi Arabia were examined, along with their effects, and solutions for a permanent solution to the problem were proposed. Cyberattacks were analyzed based on the type, source, extent, and type of information or service that was compromised. In [7], a model was presented to evaluate security risks. Essentially, it was a concept to understand and manage IT security risks comprehensively based on risk-based security management that incorporates organizational culture, knowledge, and security management. In [8], an information security policy compliance model was proposed that included variables such as resource weakness, self-efficiency, and awareness. According to the proposed model, security policy compliance is determined by three factors: self-efficiency, resource weakness, and awareness. The model suggested that when these three variables are high, compliance with security policies is more likely. Organizations should focus on increasing self-efficiency, reducing resource weakness, and increasing awareness to increase the likelihood of successful security policy compliance. In [9], a consistent framework was presented to measure the condition and suitability of the information security management frameworks of small and medium-sized organizations. However, small and medium-sized companies might not find it flexible enough to use it.

In [10], the role of secondary education in promoting information security among Saudi Arabian students was studied, as well as its realities, difficulties, and the necessary conditions for activation. The study discovered considerable discrepancies between men and women in what was needed to improve their culture. Secondary education was found to play a weak role in improving students' attitudes toward information security, but first, the necessary prerequisites must be met. In [11], cloud attacks were studied among graduate students, discovering that most attacks were related to cloud storage security concerns. It was also noted that social networking security helps and creates awareness of the necessity of social awareness programs in higher education institutions. In [12], the perspectives of IT personnel in Saudi companies were investigated. Most of the companies studied had implemented information security policies and used ethical technology, but many of these policies were not properly and efficiently enforced or made public. The study encouraged the Saudi Communications and Information Technology Commission to create a national framework for instructing companies on ethical information security procedures. In [13], a model was developed to analyze the IS success model and cybersecurity elements that affect the efficiency and use of e-Gov services in Saudi Arabia. The findings showed that the basic IS constructs had a significant impact on the satisfaction of users and the degree of danger they perceived. In [14], cybersecurity was investigated from the Saudi Arabian e-Gov projects' point of view, presenting a comprehensive approach that incorporated scientific principles. The study considered the operating environment of the project, focused on security, and claimed that cybersecurity must be developed and customized to meet the needs of citizens served by an e-Gov system.

In [15], a Cybersecurity Maturity Assessment Framework (SCMAF) was proposed for HEIs in Saudi Arabia, which was a comprehensive and customized security maturity assessment framework that can be used as a self-assessment method to establish security levels and highlight weaknesses and mitigation plans. SCMAF was implemented as a lightweight assessment tool that can be provided online or offline to ensure data privacy. In [16], the amount of data lost or stolen during data breaches was determined and the effectiveness of cybersecurity policies was investigated in companies. Multiple regression tests were used to evaluate the effectiveness of 12 cybersecurity practices in three areas for small businesses: financial loss, loss of sensitive data, and restoration time. In [17], the applicability of a theory-based model and the determinants of Information Security Compliance Behaviors (ISCB) among healthcare professionals in Saudi Arabian government hospitals were identified. The findings implied that while demographic traits have little effect on ISCB, moderating and uncommon factors, such as religion and morality, do. In [18], difficulties and impediments in security, privacy, reliability, integration, and data portability were examined in the health and patient care industries. Privacy and security issues with cloud computing and electronic health were discussed, as well as potential methods for dealing with them [19]. In [20], the security of different web applications was evaluated using a hybrid Fuzzy Analytical Hierarchy Process-Technique for Order of Preference by Similarity to Ideal Solution (Fuzzy AHP-TOPSIS) method. The study suggested integrating security in-between web application development. In [21], the present methods of the GCC countries for managing e-waste were reviewed, projecting the output until 2040 and covering the potential long-term effects on the economy, security, and ecology, suggesting steps to protect private data contained in discarded electronic components. The study recommended a thorough review of current legislation to address potential security and environmental challenges and emphasize economic opportunities.

Additionally, several studies aimed at discovering the risks for organizations. Organizations can use these studies to classify and respond to security events, mitigate risks, and expand their overall security attitude with the help of digital forensics. Numerous studies investigated and discovered incidents, data breaches, and other digital attacks on organizations [22-61]. As a result, the above review shows that Saudi Arabian organizations lack a comprehensive security framework to mitigate and avert possible risks, leading to a difficult situation in terms of monitoring, managing, and protecting all assets and resources of the organization.

III. METHODOLOGY

This study used DSM to develop a new security framework for Saudi organizations to mitigate and avoid unexpected events. DSM uses a combination of research methods to develop and test design solutions [62-63]. According to design science, research can solve design problems and improve products, services, and systems. The development process involves five steps:

- Identifying the problem
- Creating research questions
- Conducting an e-literature review
- Developing a novel security framework

- Investigating and validating the framework

A. Identifying the Problem

The purpose of this step is to identify the current problems that Saudi organizations face in the event of unexpected events or incidents. Assets may be destroyed or compromised due to such incidents. Several Saudi organizations are currently experiencing problems that may be affected by unexpected events, including the absence of disaster response plans, insufficient investment in cybersecurity, weak interior controls, lack of communication between sectors, and inadequate training and understanding of emergency response procedures.

B. Creating Research Questions

This step determines the research questions to identify the limitations and drawbacks of traditional security models for Saudi organizations. The research questions were "What security measures should Saudi organizations implement to protect confidential data and reduce the risk of data breaches?", "How do Saudi organizations protect their data?", and "What are their limitations with the existing security models?"

C. E-Literature Review

This step involved research on current security models and frameworks used by Saudi organizations. The search results included only articles published in journals and conferences between 2015 and 2023 in English. This period was selected because it ensured the availability of sufficient data. Table I summarizes the search results. The articles were filtered according to the research objectives. For this purpose, inclusion/exclusion criteria were selected. Based on the analysis of the security models and frameworks discovered, the development of a novel security framework was required to mitigate and avoid unexpected events. The proposed security framework should provide an integrated approach to security risk management, be comprehensive, and include components such as threat analysis, risk assessment, incident response, and security monitoring.

TABLE I. RESEARCH RESULTS SUMMARY

Search Engines	Keywords	Results
IEEE Explorer	Security frameworks, Security models, and Saudi organizations	89
Scopus		108
Springer		1010
Web of Science		95
Google Scholar		1503

D. Developing A Novel Security Framework

The proposed security framework for Saudi organizations consists of five steps, as shown in Figure 1: risk assessment and management, security intelligence and analysis, security policies and procedures, and security monitoring. The developed framework was based on ISO/IEC 27001:2013, NIST Cybersecurity Framework, COBIT, and the SANS Top 20 Critical Security Controls.

1) Risk Assessment and Management Stage

A process that threatens a company's earnings and capital should be identified, assessed, and controlled. This stage involves identifying potential risks, assessing their likelihood and impact, and implementing measures to reduce risks to an acceptable level. An organization's operations would not be complete without it. This minimizes the risk of unexpected losses and maximizes the success potential of the organization. In addition, it helps to comply with applicable laws. Processes, operations, and products are analyzed for potential weaknesses or vulnerabilities. Assessing risk involves determining the likelihood of an event occurring and its impact on the organization. In addition to quantitative methods, qualitative methods, such as interviews and surveys, can also be used. As a third step, develop strategies that can involve changing processes and procedures, implementing new technologies, or insurance policies. Lastly, the organization should monitor and review its strategies over time to ensure their effectiveness.

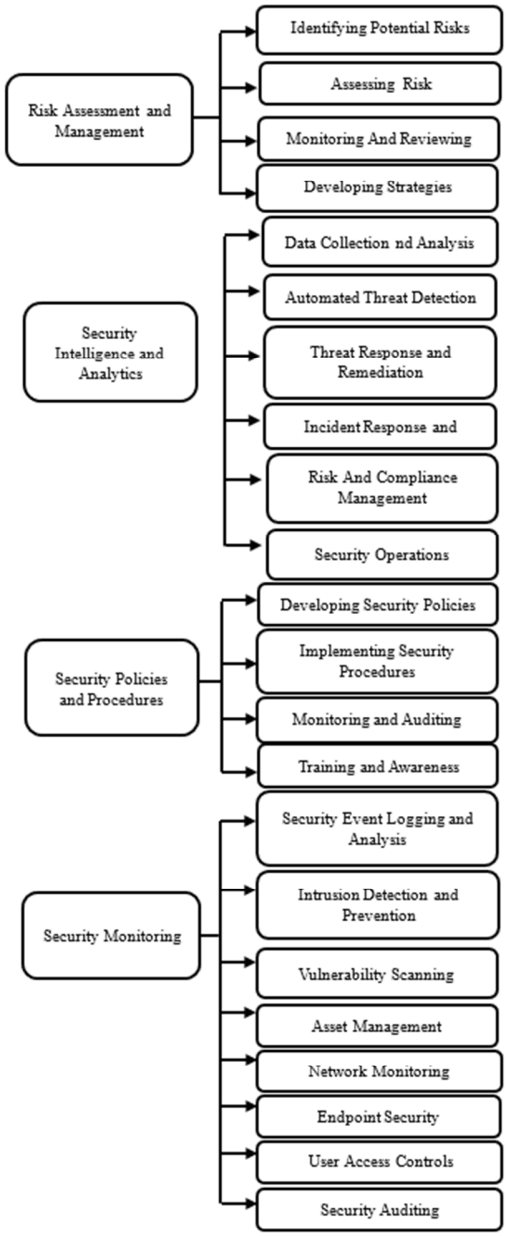

Fig. 1. The proposed security framework for Saudi organizations.

2) Security Intelligence and Analytics Stage

In this stage, information is collected, analyzed, and interpreted. Organizations can detect and respond to potential threats with a detailed understanding of their security posture. This stage consists of several steps. First, collect and analyze data from a variety of sources, such as networks, endpoints, applications, databases, and cloud services. Second, automated threat detection using advanced algorithms and machine learning techniques. It is necessary to develop and implement a threat response and restoration plan to resolve the issue. Third, incident response and forensics, in which evidence is collected and analyzed to determine the cause and scope of a security incident. Fourth, risk and compliance management helps organizations identify, assess, mitigate, and comply with applicable laws and regulations. The final step is to protect information assets through security operations.

3) Security Policies and Procedures

Organizations can develop and implement security policies and procedures tailored to their specific needs and objectives to protect information systems, networks, and other assets from risks. Four components make up this stage: First, the development of security policies helps organizations protect their assets, data, and systems, as they provide guidelines to define acceptable use of technology. The second step is to implement security procedures to ensure compliance with security policies. Authentication systems, access control systems, and encryption techniques are examples of technical controls. In the third step, security logs, reports, and user activities are reviewed and audited regularly to ensure that policies and procedures are followed and that security incidents are handled appropriately. In the final step, employees must be trained and made aware of security policies and procedures, as well as provided with resources to make them aware of risks and vulnerabilities. Security-related training and awareness campaigns should be provided regularly.

4) Security Monitoring Stage

This step aims to regularly evaluate an organization's networks, systems, and applications to ensure that there are no vulnerabilities or malicious activity present. Monitoring an organization's IT environment continuously for suspicious or harmful behavior involves continuously observing and analyzing its activities. There are eight components in this stage. First, security event logging and analysis collects and analyzes logs from various sources, such as network traffic, applications, and systems, to detect anomalies or suspicious behaviors. The second step is intrusion prevention and detection which detects and blocks malicious traffic. Third, vulnerability scanning identifies and mitigates any potential threats by regularly scanning the network for known vulnerabilities. In the fourth step, it is ensured that all assets are secure, including hardware and software. In the fifth step, network monitoring is used to detect suspicious or malicious activity. In the sixth step, endpoint security is installed and monitored on all devices to protect them from malware or malware-like attacks. The seventh step involves user access controls, which establish policies to control access to resources by ensuring that they have the necessary permissions. Finally, security auditing is performed to identify any security vulnerabilities in systems and networks.

5) Testing and Validating the Framework

The developed framework must be tested and validated to ensure its capacity and effectiveness before using it in a simulated environment. Security experts and the organization should also evaluate and validate the framework's effectiveness. Future work will implement this step.

IV. DISCUSSION

The proposed framework includes four stages: risk assessment and management, security intelligence and analytics, security policies and procedures, and security monitoring. Organizations must identify, assess, and mitigate potential risks during the risk assessment and management stage. This stage identifies potential vulnerabilities and threats, assesses their likelihood, and develops and implements security measures to mitigate them. Data must be collected and analyzed to determine potential vulnerabilities and threats. Machine learning and artificial intelligence technologies can be used to detect anomalies by monitoring network activity and analyzing user behaviors. Developing and implementing security policies and procedures that protect the organization from potential threats and vulnerabilities is the goal of the policy and procedures stage. This stage also includes policies for access control, user authentication, and encryption. Lastly, security monitoring involves monitoring any suspicious activity within the organization's systems. Monitoring user behavior and reviewing access control policies are some of the steps involved in this stage. The proposed security framework provides a comprehensive approach to protect the organization from potential threats and vulnerabilities. As part of the security process, the organization's systems are monitored for suspicious activity and identified, assessed, and mitigated risks. This security framework was developed using ISO/IEC 27001:2013, the NIST Cybersecurity Framework, and COBIT, which are three common security frameworks. The proposed model may also work with organizations in other countries than Saudi Arabia, as it is built based on these common security frameworks. For instance, risk assessment and management are provided by the NIST framework, security intelligence and analytics are provided by the COBIT framework, and ISO / IEC 27001:2013 was used for developing security policies and procedures.

V. CONCLUSION

This study proposed a security framework for Saudi organizations to mitigate and avoid unexpected security events. The proposed framework was based on ISO/IEC 27001:2013, the NIST Cybersecurity Framework, and COBIT, and included four stages: risk assessment and management, security intelligence and analysis, security policies and procedures, and security monitoring. The proposed framework can also be applied in organizations of other countries, as it is based on three common security frameworks.

REFERENCES

[1] R. Saint-Germain, "Information security management best practice based on ISO/IEC 17799; the international information security standard

provides a framework for ensuring business continuity, maintaining legal compliance, and achieving a competitive edge," *Information Management Journal*, vol. 39, no. 4, pp. 60–66, Jul. 2005.

[2] Lynette Mears and R. von Solms, "Corporate Information Security Governance: A Holistic Approach," presented at the ISSA 2004 enabling tomorrow Conference, Johannesburg, South Africa, 2004.

[3] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," in *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, Bangkok, Thailand, Jan. 2023, pp. 117–122, https://doi.org/10.1109/CyMaEn57228.2023.10051114.

[4] P. Radanliev, "Review and Comparison of US, EU, and UK Regulations on Cyber Risk/Security of the Current Blockchain Technologies: Viewpoint from 2023," *The Review of Socionetwork Strategies*, May 2023, https://doi.org/10.1007/s12626-023-00139-x.

[5] Lilis Griffith Toyner; Sfenrianto Sfenrianto, "Information System Security Evaluation Using COBIT 5 Framework," *Journal of Information System Management (JOISM)*, vol. 4, no. 2, pp. 147–157, 2023.

[6] M. Alsaif, N. Aljaafari, and A. R. Khan, "Information Security Management in Saudi Arabian Organizations," *Procedia Computer Science*, vol. 56, pp. 213–216, Jan. 2015, https://doi.org/10.1016/j.procs.2015.07.201.

[7] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information systems security policies: a contextual perspective," *Computers & Security*, vol. 24, no. 3, pp. 246–260, May 2005, https://doi.org/10.1016/j.cose.2004.08.011.

[8] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model of Information Security Policy Compliance," vol. 42, no. 1, pp. 285–311, 2018, https://doi.org/10.25300/MISQ/2018/13853.

[9] L. Kaušpadienė, S. Ramanauskaitė, and A. Čenys, "Information security management framework suitability estimation for small and medium enterprise," *Technological and Economic Development of Economy*, vol. 25, no. 5, pp. 979–997, Jun. 2019, https://doi.org/10.3846/tede.2019.10298.

[10] D. M. A. Hassan, "The Role of Secondary Education in Enhancing the Information Security Culture among Students in Saudi Arabia," *Journal of Positive Psychology and Wellbeing*, vol. 6, no. 2, pp. 1782–1796, Sep. 2022.

[11] "Information Security Issues and Threats in Saudi Arabia: A Research Survey," *International Journal of Computer Science Issues*, vol. 13, no. 6, pp. 129–135, Nov. 2016, https://doi.org/10.20943/01201606.129135.

[12] Z. A. Alzamil, "Information security practice in Saudi Arabia: case study on Saudi organizations," *Information & Computer Security*, vol. 26, no. 5, pp. 568–583, Jan. 2018, https://doi.org/10.1108/ICS-01-2018-0006.

[13] M. S. Al-Zahrani, "Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 4937–4955, Oct. 2020, https://doi.org/10.11591/ijece.v10i5.pp4937-4955.

[14] A. Alrubaiq and T. Alharbi, "Developing a Cybersecurity Framework for e-Government Project in the Kingdom of Saudi Arabia," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 302–318, Jun. 2021, https://doi.org/10.3390/jcp1020017.

[15] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Computer Science*, vol. 7, Sep. 2021, Art. no. e703, https://doi.org/10.7717/peerj-cs.703.

[16] F. Alharbi *et al.*, "The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia," *Sensors*, vol. 21, no. 20, Jan. 2021, Art. no. 6901, https://doi.org/10.3390/s21206901.

[17] S. T. Alanazi, M. Anbar, S. A. Ebad, S. Karuppayah, and H. A. Al-Ani, "Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector," *Symmetry*, vol. 12, no. 9, Sep. 2020, Art. no. 1544, https://doi.org/10.3390/sym12091544.

[18] E. Chikhaoui, J. Sarabdeen, and R. Parveen, "Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia," *Communications of the IBIMA*, vol. 2017, pp. 1–18, May 2017, https://doi.org/10.5171/2017.369309.

[19] M. Rasool, N. A. Ismail, A. Al-Dhaqm, W. M. S. Yafooz, and A. Alsaeedi, "A Novel Approach for Classifying Brain Tumours Combining a SqueezeNet Model with SVM and Fine-Tuning," *Electronics*, vol. 12, no. 1, Jan. 2023, Art. no. 149, https://doi.org/10.3390/electronics12010149.

[20] A. Agrawal *et al.*, "Evaluating the Security Impact of Healthcare Web Applications Through Fuzzy Based Hybrid Approach of Multi-Criteria Decision-Making Analysis," *IEEE Access*, vol. 8, pp. 135770–135783, 2020, https://doi.org/10.1109/ACCESS.2020.3010729.

[21] J. Alghazo, O. K. M. Ouda, and A. E. Hassan, "E-waste environmental and information security threat: GCC countries vulnerabilities," *Euro-Mediterranean Journal for Environmental Integration*, vol. 3, no. 1, p. 13, Jan. 2018, https://doi.org/10.1007/s41207-018-0050-4.

[22] A. M. R. Al- Dhaqm, S. H. Othman, S. Abd Razak, and A. Ngadi, "Towards adapting metamodelling technique for database forensics investigation domain," in *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, Kuala Lumpur, Malaysia, Dec. 2014, pp. 322–327, https://doi.org/10.1109/ISBAST.2014.7013142.

[23] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R. Kebande, and S. Hajar Othman, "Face Validation of Database Forensic Investigation Metamodel," *Infrastructures*, vol. 6, no. 2, Feb. 2021, Art. no. 13, https://doi.org/10.3390/infrastructures6020013.

[24] A. Al-Dhaqm *et al.*, "Digital Forensics Subdomains: The State of the Art and Future Directions," *IEEE Access*, vol. 9, pp. 152476–152502, 2021, https://doi.org/10.1109/ACCESS.2021.3124262.

[25] A. Aldhaqm, S. A. Razak, and S. H. Othman, "Common investigation process model for database forensic investigation discipline," presented at the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia, Apr. 2015.

[26] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field," *Computational Intelligence and Neuroscience*, vol. 2022, Feb. 2022, Art. no. e8002963, https://doi.org/10.1155/2022/8002963.

[27] F. M. Ghabban, I. M. Alfadli, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Comparative Analysis of Network Forensic Tools and Network Forensics Processes," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Cameron Highlands, Malaysia, Jun. 2021, pp. 78–83, https://doi.org/10.1109/ICSCEE50312.2021.9498226.

[28] O. Ameerbakhsh, F. M. Ghabban, I. M. Alfadli, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Digital Forensics Domain and Metamodeling Development Approaches," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Cameron Highlands, Malaysia, Jun. 2021, pp. 67–71, https://doi.org/10.1109/ICSCEE50312.2021.9497935.

[29] A. A. Alhussan, A. Al-Dhaqm, W. M. S. Yafooz, A. H. M. Emara, S. Bin Abd Razak, and D. S. Khafaga, "A Unified Forensic Model Applicable to the Database Forensics Field," *Electronics*, vol. 11, no. 9, Jan. 2022, Art. no. 1347, https://doi.org/10.3390/electronics11091347.

[30] F. M. Alotaibi, A. Al-Dhaqm, Y. D. Al-Otaibi, and A. A. Alsewari, "A Comprehensive Collection and Analysis Model for the Drone Forensics Field," *Sensors*, vol. 22, no. 17, Jan. 2022, Art. no. 6486, https://doi.org/10.3390/s22176486.

[31] W. M. S. Yafooz, A. Al-Dhaqm, and A. Alsaeedi, "Detecting Kids Cyberbullying Using Transfer Learning Approach: Transformer Fine-Tuning Models," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 255–267.

[32] A. A. Alhussan, A. Al-Dhaqm, W. M. S. Yafooz, S. B. A. Razak, A.-H. M. Emara, and D. S. Khafaga, "Towards Development of a High Abstract Model for Drone Forensic Domain," *Electronics*, vol. 11, no. 8, Jan. 2022, Art. no. 1168, https://doi.org/10.3390/electronics11081168.

[33] I. M. Alfadli, F. M. Ghabban, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "CIPM: Common Identification

Process Model for Database Forensics Field," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Cameron Highlands, Malaysia, Jun. 2021, pp. 72–77, https://doi.org/10.1109/ICSCEE50312.2021.9498014.

[34] S. Abd Razak, N. H. Mohd Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," *IEEE Access*, vol. 8, pp. 43256–43264, 2020, https://doi.org/10.1109/ACCESS.2020.2977117.

[35] A. Al-Dhaqm, S. H. Othman, W. M. S. Yafooz, and A. Ali, "Review of Information Security Management Frameworks," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 69–80.

[36] M. Salem, S. H. Othman, A. Al-Dhaqm, and A. Ali, "Development of Metamodel for Information Security Risk Management," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 243–253.

[37] A. Al-Dhaqm, W. M. S. Yafooz, S. H. Othman, and A. Ali, "Database Forensics Field and Children Crimes," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 81–92.

[38] M. Saleh *et al.*, "A Metamodeling Approach for IoT Forensic Investigation," *Electronics*, vol. 12, no. 3, Jan. 2023, Art. no. 524, https://doi.org/10.3390/electronics12030524.

[39] A. Ali, S. A. Razak, S. H. Othman, R. R. Marie, A. Al-Dhaqm, and M. Nasser, "Validating Mobile Forensic Metamodel Using Tracing Method," in *Advances on Intelligent Informatics and Computing*, 2022, pp. 473–482, https://doi.org/10.1007/978-3-030-98741-1_39.

[40] D. S. A. Baras, S. H. Othman, A. Al-Dhaqm, and R. Z. R. M. Radzi, "Information Security Management Metamodel (ISMM) Validation and Verification through Frequency-based Selection Technique," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, Bandung, Indonesia, Jul. 2021, pp. 292–297, https://doi.org/10.1109/ICoDSA53588.2021.9617527.

[41] A. M. R. Al-Dhaqm, "Simplified Database Forensic Investigation Using Metamodeling Approach," Ph.D. dissertation, Universiti Teknologi Malaysia, Skudai, Malaysia, 2019.

[42] V. R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, Dec. 2016, pp. 356–362, https://doi.org/10.1109/FiCloud.2016.57.

[43] V. Kebande and H. Venter, "Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution," in *Proceedings of the 11th International Conference on Cyber Warfare and Security*, Boston, MA, USA, Mar. 2016, pp. 399–406.

[44] V. R. Kebande and H. S. Venter, "A comparative analysis of digital forensic readiness models using CFRaaS as a baseline," *WIREs Forensic Science*, vol. 1, no. 6, 2019, Art. no. e1350, https://doi.org/10.1002/wfs2.1350.

[45] A. Al-Dhaqm, S. Razak, and S. H. Othman, "Model Derivation System to Manage Database Forensic Investigation Domain Knowledge," in *2018 IEEE Conference on Application, Information and Network Security (AINS)*, Langkawi, Malaysia, Aug. 2018, pp. 75–80, https://doi.org/10.1109/AINS.2018.8631468.

[46] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020, https://doi.org/10.1109/ACCESS.2020.3014615.

[47] A. Al-Dhaqm *et al.*, "Categorization and Organization of Database Forensic Investigation Processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020, https://doi.org/10.1109/ACCESS.2020.3000747.

[48] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, pp. 145018–145032, 2020, https://doi.org/10.1109/ACCESS.2020.3008696.

[49] V. R. Kebande, R. A. Ikuesan, N. M. Karie, S. Alawadi, K.-K. R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," *Forensic Science International: Reports*, vol. 2, Dec. 2020, Art. no. 100122, https://doi.org/10.1016/j.fsir.2020.100122.

[50] V. R. Kebande, R. A. Ikuesan, and N. M. Karie, "Review of Blockchain Forensics Challenges," in *Blockchain Security in Cloud Computing*, K. M. Baalamurugan, S. R. Kumar, A. Kumar, V. Kumar, and S. Padmanaban, Eds. Cham, Switzerland: Springer International Publishing, 2022, pp. 33–50.

[51] V. R. Kebande and K.-K. R. Choo, "Finite state machine for cloud forensic readiness as a service (CFRaaS) events," *Security And Privacy*, vol. 5, no. 1, 2022, Art. no. e182, https://doi.org/10.1002/spy2.182.

[52] S. Makura, H. S. Venter, V. R. Kebande, N. M. Karie, R. A. Ikuesan, and S. Alawadi, "Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring," *Security and Privacy*, vol. 4, no. 3, 2021, Art. no. e149, https://doi.org/10.1002/spy2.149.

[53] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," *WIREs Forensic Science*, vol. 2, no. 5, 2020, Art. no. e1372, https://doi.org/10.1002/wfs2.1372.

[54] A. E. Yahya, A. Gharbi, W. M. S. Yafooz, and A. Al-Dhaqm, "A Novel Hybrid Deep Learning Model for Detecting and Classifying Non-Functional Requirements of Mobile Apps Issues," *Electronics*, vol. 12, no. 5, Jan. 2023, Art. no. 1258, https://doi.org/10.3390/electronics12051258.

[55] R. Al-Mugerrn, A. Al-Dhaqm, and S. H. Othman, "A Metamodeling Approach for Structuring and Organizing Cloud Forensics Domain," in *2023 International Conference on Smart Computing and Application (ICSCA)*, Hail, Saudi Arabia, Oct. 2023, pp. 1–5, https://doi.org/10.1109/ICSCA57840.2023.10087425.

[56] A. Aldhaqm, S. A. Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 12, no. 4, pp. 386–394, 2016, https://doi.org/10.19026/rjaset.12.2377.

[57] A. M. R. Al-Dhaqm and M. A. Nagdi, "Detection and Prevention of Malicious Activities on RDBMS Relational Database Management Systems," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, Sep. 2012.

[58] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Extraction of Common Concepts for the Mobile Forensics Domain," in *Recent Trends in Information and Communication Technology*, Johor Bahru, Malaysia, 2018, pp. 141–154, https://doi.org/10.1007/978-3-319-59427-9_16.

[59] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Towards Adapting Metamodeling approach for the Mobile Forensics Investigation Domain," presented at the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia, 2015.

[60] M. A. Saleh, S. Hajar Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common Investigation Process Model for Internet of Things Forensics," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Cameron Highlands, Malaysia, Jun. 2021, pp. 84–89, https://doi.org/10.1109/ICSCEE50312.2021.9498045.

[61] B. Zawali, R. A. Ikuesan, V. R. Kebande, S. Furnell, and A. A-Dhaqm, "Realising a Push Button Modality for Video-Based Forensics," *Infrastructures*, vol. 6, no. 4, Apr. 2021, https://doi.org/10.3390/infrastructures6040054.

[62] J. F. Wolfswinkel, E. Furtmueller, and C. P. M. Wilderom, "Using grounded theory as a method for rigorously reviewing literature," *European Journal of Information Systems*, vol. 22, no. 1, pp. 45–55, Jan. 2013, https://doi.org/10.1057/ejis.2011.51.

[63] A. Al-Dhaqm *et al.*, "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017, https://doi.org/10.1109/ACCESS.2017.2762693.