Digital Forensics Readiness Framework (DFRF) to Secure Database Systems

Ahmed Albugmi
Computer and Information Technology Department, The Applied College, King Abdulaziz University, Saudi Arabia
analbogome@kau.edu.sa (corresponding author)

Received: 21 February 2024 | Revised: 2 March 2024 | Accepted: 10 March 2024

ABSTRACT

Database systems play a significant role in structuring, organizing, and managing data of organizations. In this regard, the key challenge is how to protect the confidentiality, integrity, and availability of database systems against attacks launched from within and outside an organization. To resolve this challenge, different database security techniques and mechanisms, which generally involve access control, database monitoring, data encryption, database backups, and strong passwords have been proposed. These techniques and mechanisms have been developed for certain purposes but fall short of many industrial expectations. This study used the design science research method to recommend a new Digital Forensic Readiness Framework, named DFRF, to secure database systems. DFRF involves risk assessments, data classification, database firewalls, data encryption, strong password policies, database monitoring and logging, data backups and recovery, incident response plans, forensic readiness, as well as education and awareness. The proposed framework not only identifies threats and responds to them more effectively than existing models, but also helps organizations stay fully compliant with regulatory requirements and improve their security. The design of the suggested framework was compared with existing models, confirming its superiority.

Keywords-database systems; digital forensics; forensic readiness; design science method

I. INTRODUCTION

In general, Database Management Systems (DBMS) help create, modify, share, and manage database transactions among users and applications [1-2]. These systems have several advantages as they help separate user applications from the underlying physical databases and facilitate the use and management of the actual database. Despite their numerous benefits, these systems have also some disadvantages. Several attacks can compromise the integrity, confidentiality, and availability of databases [3-4]. The security measures of databases are continuously improved despite the increasing complexity of attacks. For this reason, many traditional security measures were suggested, including using secure and strong passwords, controlling access to data, encrypting data, performing database backups, and monitoring databases. Although these measures are effective under some conditions, some limitations, such as the use of weak passwords, inadequate encryption of the data, and risky behavior of users, still exist. Organizations must use digital evidence as effectively as possible to meaningfully reduce investigation costs [5]. Companies need to expand their forensic capabilities, establish efficient processes for collecting and preserving data, make effective collaborations with external experts, and employ high-standard investigative methods to have more rapid and efficient forensic investigations. This study applies the Design Science Research Methodology (DSRM) to design a digital forensic readiness framework, named DFRF, to ensure database security. This framework is expected to help organizations identify and competently deal with the security challenges that can arise in digital databases. A key objective of DFRF is the identification and mitigation of database vulnerabilities. This framework performs periodic assessments and audits to unveil any weaknesses that may exist in a system's configuration, access control, and data encryption measures. Successfully managing these problems, minimizing the risk of data breaches, securing databases, and preventing data breaches could result in a significant decrease in database security risks.

II. RELATED WORKS

Several studies have argued that database security models might fail when applied [6-11]. DBMSs differ greatly in terms of functionality, which may explain this failure. In addition, database forensics is focused on one dimension (file system), which primarily involves identifying, gathering, handling, storing, responding to incidents, and training. However, in some cases, it is possible to trace database incidents when digital investigators cooperate to analyze the database [8]. Owing to the multidimensionality and diversity of DBMSs, it is difficult to develop a standardized approach to database forensics. Current digital forensic models do not cover the full range of database concepts [12]. According to [13-14], most of the studies on database forensics focused on resolving database contents and metadata, which is consistent with documents rather than database incidents. In [13], it was shown that investigation processes can be utilized to collect data related to operations executed using Oracle database concepts by performing certain tasks. Also, four steps were proposed to resolve the problem: reconstructing databases, canceling database operations, collecting data, and repairing integrity issues. In [15], an audit reconstruction tool was presented to extract information from logs when auditing features are disabled. The Oracle database has been the subject of several forensic investigation models. For example, in [15], it was displayed how an Oracle log file can be used to detect attack events by examining the binary format of redo logs. Furthermore, it was demonstrated how attackers conceal their tracks after a failed attack, as well as the way to detect them. According to [16], evidence that has already been deleted could be recovered in the case of Oracle objects, and data files extracted from a compromised server can be indirectly recovered by investigators using this procedure. Additionally, malicious entities can drop objects. The listener's log file and audit trail can be put into service to capture evidence of attacks against the authentication mechanism. An instance name and the IP address of the server are also recorded in this log file, along with the Service Identifier (SID) and the IP address of the connection. On the contrary, the audit trail can indicate whether a log-in or log-out was successful or unsuccessful. The listener log file and audit trails can be used by investigators to collect evidence against the authentication mechanism, but first, the respective database must be configured with an audit trail enabled.

In [17], a forensic model in which the database servers are disconnected from the network to capture volatile data was proposed. The recommended evidence collection and identification processes can be employed to retrieve fragile data from the database server. Forensic techniques are applied to move the captured data once the server is disconnected from the network and the forensic environment. A compromised database server is obtained for evidence collection in the evidence collection process. The recovery and careful storage of volatile data is necessary for forensic research. A human-readable form makes it easier for forensic inspectors to examine non-volatile data, as opposed to stored binary forms. In [18], a detection investigation model was presented to help the examiner find evidence of data theft. A DBA or incident responder can use the model to determine whether such a breach has occurred in a situation where no audit trail exists, but the assumption is that unauthorized access has been obtained to the data on the server. In [19], a forensic analysis method was proposed for MSSQL servers, consisting of four phases: preparation of the investigation, verification of the incident, collection of artifacts, and analysis. In [20], another model was proposed to detect and investigate database servers. It involved three phases: server detection, data collection, and data analysis, but this model cannot handle volatile artifacts. In [21], a database model was introduced to identify and name inconsistencies in the MySQL database system. In [22], a reconstruction model was developed to restore already deleted or updated values from redo logs to reconstruct basic SQL statements. The basic DDL statement was overlooked in this proposed model, as it was based on the DML statements. In [23], a practical forensic method was discussed to reconstruct basic SQL DDL statements and improve the previous method. In [14], a framework was showcased to identify, collect, analyze, validate, and document digital evidence that has been altered. This framework collected, analyzed, and reconstructed volatile and non-volatile data.

In addition to the different forensic tamper detection and analysis algorithms proposed for DBMSs, several forensic tamper detection models have also been suggested. In [24], methods and scenarios were recommended to detect covert databases. In [25], a model was proposed to efficiently collect digital evidence. This study stated that a database business environment could gather evidence against authorized and unauthorized events using triggers, replication, and log file backup. In [26], a forensic tamper detection model was introduced deploying a one-way hash function that could detect compromised audit logs. However, this model could not detect when tampering occurred, which data were altered, and the identity of the attacker, as it was not able to analyze intruder activities. In [7], a model was introduced to investigate compromised databases by involving two examination processes: identification and collection. In [27], a method was presented to collect, preserve, and analyze database metadata to prevent attacks on databases using four investigation processes: collecting and preserving evidence, analyzing anti-forensic attacks, analyzing database attacks, and preserving evidence reports. In [28], it was attempted to reconstruct database events to uncover intruders' actions by collecting and reconstructing evidence. In [12], forensic investigation frameworks were developed for NoSQL DBMSs based on their unique features. This process involved five parallel phases: preparation, acquisition and preservation, identification of distributed evidence, examination and analysis, and finally reporting and presentation. The framework did not include database schemes' evaluation or analysis of database characteristics, such as gathering logs for assessing operations. In [29], MongoDB was studied, which is among the most widely employed NoSQL DBMSs, and a forensic tool was proposed to explore the internal structure and format of the data files. In [30], a comprehensive review of database forensic investigation processes was presented to help domain researchers gain a deeper understanding of database forensics from various perspectives. This study also discussed the issues and drawbacks that emerged and proposed solutions. In [31], database forensic models proposed from 2009 to 2015 were evaluated but did not address limitations, challenges, issues, directions, or proposed solutions for database forensics. In [32], another review was conducted for the period 2015-2017 in database forensics. For the database forensics field, five stages of forensic analysis were proposed: determining, examining, presenting, documenting, and reporting the event.

III. METHODOLOGY

This study aimed to design a digital forensics readiness framework to secure database systems using the DSRM, which is suitable for designing and validating artifices in a digital forensics context. DSRM was utilized as the analysis method for several reasons: 1) It is a solution-oriented analysis method that is deployed to produce logical, testable, and communicable products, 2) the formal process it follows facilitates the research procedure, and 3) ensures the smooth, cohesive link between the design and development of the model and its evaluation and demonstration. Figure 1 displays the adapted DSRM and the operational framework. DSRM consists of the following four stages.

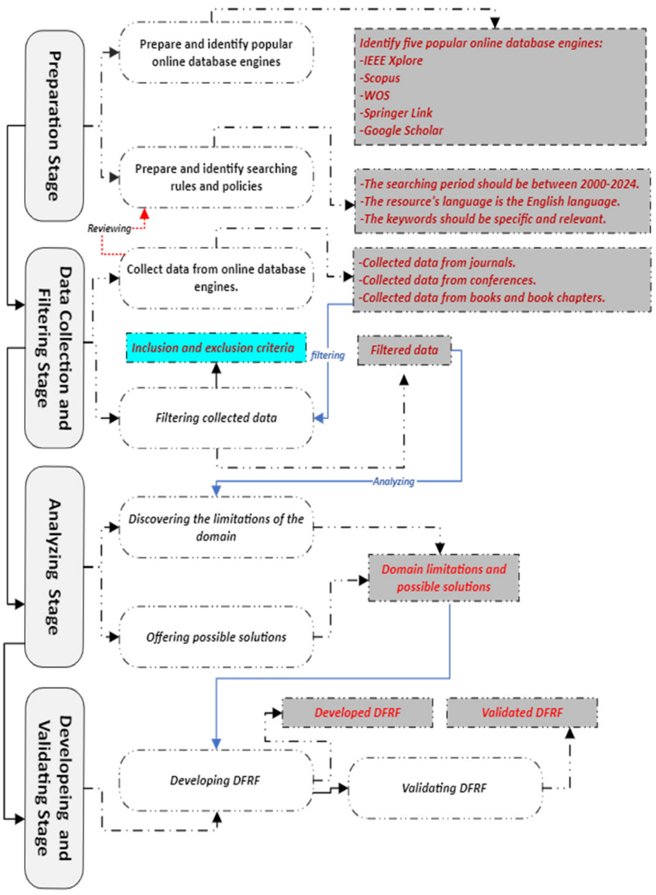
Preparation Stage
Prepare and identify popular online database engines
Identify five popular online database engines:
-IEEE Xplore
-Scopus
-WOS
-Springer Link
-Google Scholar
Prepare and identify searching rules and policies
-The searching period should be between 2000-2024.
-The resource's language is the English language.
-The keywords should be specific and relevant.
Reviewing
Data Collection and Filtering Stage
Collect data from online database engines.
-Collected data from journals.
-Collected data from conferences.
-Collected data from books and book chapters.
Inclusion and exclusion criteria
filtering
Filtered data
Filtering collected data
Analyzing
Analyzing Stage
Discovering the limitations of the domain
Domain limitations and possible solutions
Offering possible solutions
Developing and Validating Stage
Developed DFRF
Validated DFRF
Developing DFRF
Validating DFRF

Fig. 1. Adapted DSRM and operational framework.

A. Preparation

This stage prepares the search guidelines that will govern and control the research process and consists of two parts: identifying popular online databases and determining the rules for the search procedure. For the first part, five online databases were identified: IEEE Xplore, Scopus, Web of Science (WOS), Springer Link, and Google Scholar. For the second part, three rules were set: a) the search period was set to be from 2000 to 2024, b) the language of the resource should be English, and c) the keywords were: "digital forensic", "forensics readiness", "database forensic", and "database systems".

B. Data Collection and Filtering

This stage aimed to collect and filter the data gathered in the previous stage. Figures 2-5 show the data collected from the above databases based on the defined keywords.

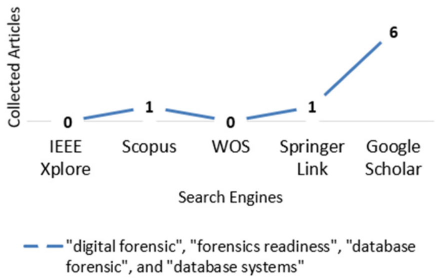

Fig. 2. Collected data based on all four keywords.

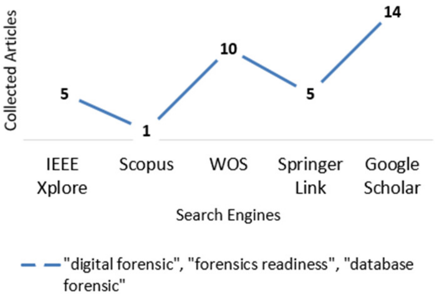

Fig. 3. Collected data based on three keywords.

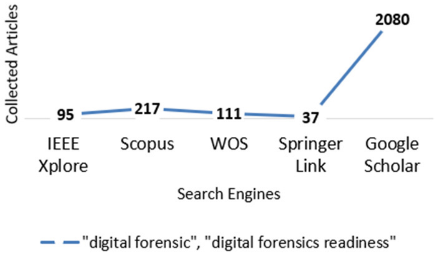

Fig. 4. Collected data based on two keywords.

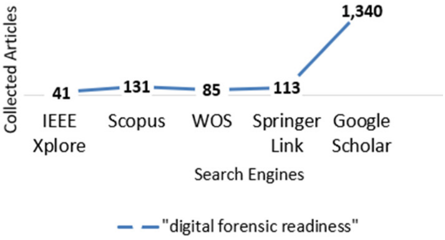

Fig. 5. Collected data based on one keyword.

These results helped to determine the direction of the research and the attention and motivation of the researchers. Therefore, this study did not pay more attention to database systems from a digital forensic perspective but focused instead on identifying the reasons behind this limitation in studies on database systems and database forensics. Table I presents the digital forensic models that concentrate on database systems and the way they could be implemented. As a result, a total of 57 digital forensic models, frameworks, approaches, techniques, tools, and algorithms, which were purely related to database systems, were identified. There was only one model that focused on forensic readiness for database systems [33].

TABLE I. DIGITAL FORENSIC MODELS FOCUSED ON DATABASE SYSTEMS

ID	**Year**	**Ref**	**Forensic Readiness**	**Investigation Processes**			
				Identification	**Collection and Preservation**	**Analysis & Examination**	**Presentation & Documentation**
	2004	[13]	×	√	√	√	×
	2004	[34]	×	×	×	√	×
	2006	[35]	×	√	×	×	×
	2007	[2]	×	√	×	√	×
	2007	[36]	×	√	×	×	×
	2007	[24]	×	√	×	×	×
	2007	[15]	×	×	×	√	×
	2007	[16]	×	×	×	√	×
	2007	[30]	×	×	×	√	×
	2007	[31]	×	×	×	√	×
	2007	[32]	×	×	×	√	×
	2008	[19]	×	√	√	√	√
	2008	[37]	×	×	×	√	×
	2009	[38]	×	×	×	√	×
	2009	[39]	×	×	×	√	×
	2010	[21]	×	√	×	×	×
	2011	[40]	×	√	×	×	×
	2011	[41]	×	×	√	×	×
	2011	[20]	×	√	√	√	×
	2011	[42]	×	×	×	√	×
	2012	[43]	×	√	×	×	×
	2012	[14]	×	√	√	√	√
	2012	[6]	×	√	√	√	×
	2012	[44]	×	×	×	√	×
	2012	[45]	×	×	×	√	×
	2012	[22]	×	×	√	√	×
	2012	[46]	×	×	×	√	×
	2013	[47]	×	×	×	√	×
	2013	[48]	×	×	√	√	×
	2013	[49]	×	×	×	√	×
	2013	[50]	×	×	×	√	×
	2013	[51]	×	×	×	√	×
	2013	[52]	×	×	×	√	×
	2013	[53]	×	×	×	√	×
	2013	[54]	×	×	×	√	×
	2013	[23]	×	×	×	√	×
	2014	[55]	×	×	×	√	×
	2014	[27]	×	×	×	×	×
	2014	[56]	×	×	×	×	×
	2014	[7]	×	√	√	×	×
	2014	[28]	×	×	√	√	×
	2014	[57]	×	×	×	√	×
	2015	[58]	×	×	×	√	×
	2015	[59]	×	×	×	√	×
	2015	[60]	×	×	×	√	×
	2016	[61]	×	×	×	√	×
	2016	[62]	×	√	√	√	√
	2016	[8]	×	√	√	√	√
	2017	[63]	×	×	×	√	×
	2017	[64]	×	√	√	√	√
	2017	[65]	×	√	√	√	√
	2018	[66]	×	√	√	√	√
	2019	[67]	×	√	√	√	√
	2020	[33]	√	√	√	√	√
	2020	[68]	×	√	√	√	√
	2021	[69]	×	×	×	√	×

C. *DFRF Development*

The development and validation of DFRF require the identification and selection of models from Table I based on the development criteria. This table summarizes several digital forensic models for database systems. Coverage factors were selected based on [70-71]. It is essential to cover a wide range of investigation processes to meet the development objective of the DFRF. A model is said to be well covered (i.e., it has a high coverage value) if it can incorporate all the four investigation processes mentioned in Table I. The coverage value of the model will be lower if it merely describes three or two investigation processes. As a result, this study identified two categories of models for developing and validating the proposed framework. Models related to the four different investigation processes are included in the first group. It is also possible to find models that cover three or two investigation processes in the second group. Consequently, and based on this categorization, this study found 11 models that met the first group, while eight models represented the second group. Tables II and III portray the selected development and validation models, respectively, which have redundant and overlapped investigation processes and concepts for investigation.

The common investigation procedures and concepts of digital forensics were collected from the 11 selected models on the basis of the criteria adapted from [68, 70]. In general, the investigation processes and concepts were extracted from the diagram or the main textual models. To understand the purpose and meaning of an investigation process and concept, a definition, activity, or task is also necessary. Investigation processes and concepts that were not relevant to the investigation were excluded. However, as part of the model, implicit and explicit investigation processes and concepts were included. The extracted investigations and concepts represent the input and output of the DFRF to secure database systems. The relationships between the extracted components were examined to ensure their applicability to the development process of the DFRF. Figure 6 illustrates the proposed DFRF system for securing database systems. It consists of 10 primary components: risk assessment, data classification, data encryption, database firewalls, strong password policies, database monitoring and logging, data backups and recovery, incident response plans, forensic readiness, education, and awareness.

1) *Risk Assessment*

Risk assessment refers to the identification of potential risks and weaknesses in a system and the measurement of the potential impacts of each risk. By taking this step into action, organizations would be able to properly distribute the available resources and also prioritize their efforts when mitigating the risks. An example of assessing risks in a database system is the identification and evaluation of the potential impacts of unauthorized access to or misuse of sensitive customer data. Through the assessment of the risks that may arise because of this vulnerability, companies can have a deep insight into the best security measures to take, for example, using strong password policies and/or applying suitable techniques for encrypting the data.

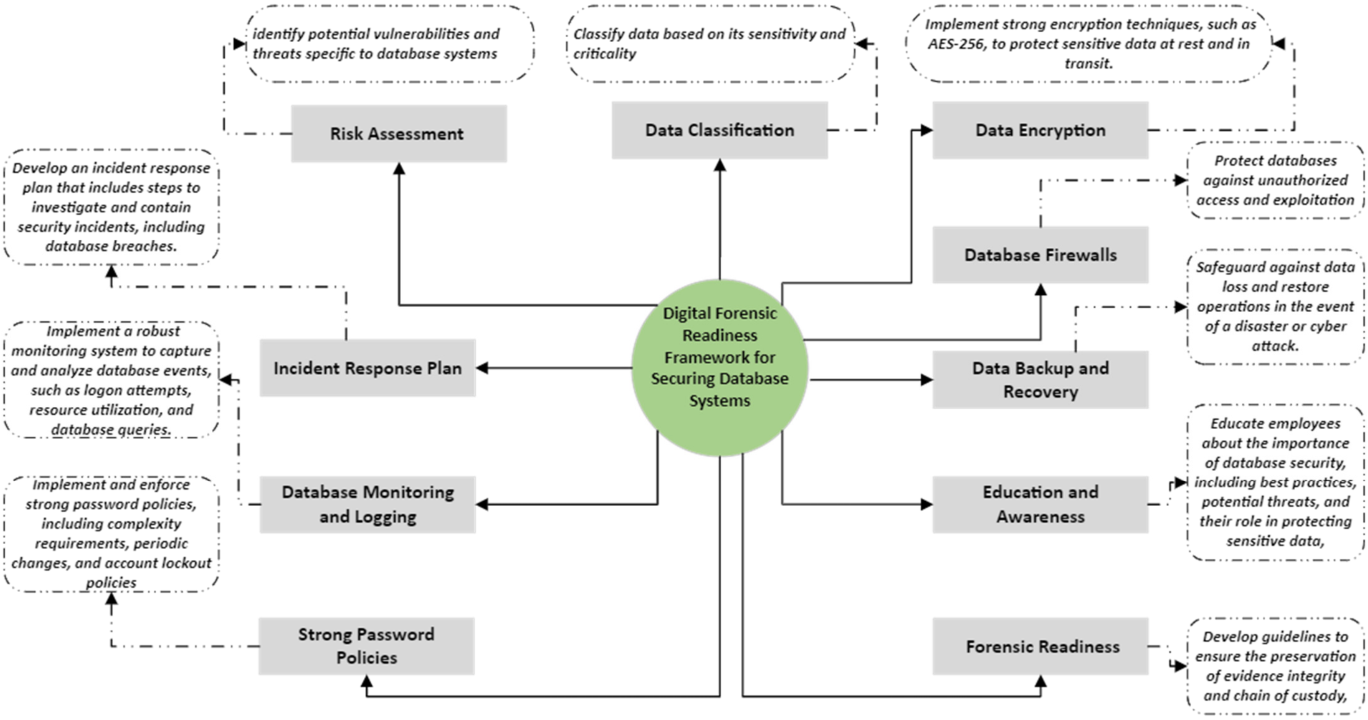
identify potential vulnerabilities and threats specific to database systems
Classify data based on its sensitivity and criticality
Implement strong encryption techniques, such as AES-256, to protect sensitive data at rest and in transit.
Risk Assessment
Data Classification
Data Encryption
Develop an incident response plan that includes steps to investigate and contain security incidents, including database breaches.
Protect databases against unauthorized access and exploitation
Database Firewalls
Safeguard against data loss and restore operations in the event of a disaster or cyber attack.
Digital Forensic Readiness Framework for Securing Database Systems
Implement a robust monitoring system to capture and analyze database events, such as logon attempts, resource utilization, and database queries.
Incident Response Plan
Data Backup and Recovery
Implement and enforce strong password policies, including complexity requirements, periodic changes, and account lockout policies
Database Monitoring and Logging
Education and Awareness
Educate employees about the importance of database security, including best practices, potential threats, and their role in protecting sensitive data,
Strong Password Policies
Forensic Readiness
Develop guidelines to ensure the preservation of evidence integrity and chain of custody,

Fig. 6. DFRF design for securing database systems.

2) Data Classification

This step involves categorizing the data according to their importance and sensitivity. Data classification helps companies identify and protect data of the highest criticality and sensitivity, allowing users to manage less sensitive data with less rigorous security measures. Actual instances of data classification in a database system are the identification and labeling of customer data, financial records, or intellectual property. Data classification helps companies ensure that proper security measures are performed for the protection of the high-sensitive data while allowing more flexible treatment with data of lower criticality.

3) Data Encryption

This process converts data into unreadable codes, known as ciphertext, with the help of a key, and only authorized parties can decipher it. Data encryption protects the data against unauthorized access, even in the case of compromise of the underlying database system. An example of data encryption in a database system is to encrypt sensitive personal data, such as financial information or social security numbers. This helps companies prevent unauthorized parties from gaining access or misusing the data, even if the underlying database system is compromised.

4) Database Firewalls

Firewalls add another layer of protection to database systems. Not only do they build a barrier between the databases themselves and an external network, but also monitor and analyze network traffic to prevent unauthorized access to data or malevolent activities. It is well exemplified using a web application firewall. This type of firewall is responsible for monitoring incoming HTTP requests and then filtering any suspicious activities. It could protect the underlying database against any potential attacks.

5) Strong Password Policies

Such policies prevent unauthorized parties from having access to database systems. Companies need to ask their users to set passwords of high complexity and uniqueness, change them regularly, and protect them from others' access. An example is to ask users to choose passwords of at least eight characters that include numbers, both uppercase and lowercase letters, and special characters. In addition, organizations could ask their users to regularly change their passwords so that any unauthorized access could be obstructed.

6) Database Monitoring and Logging

This activity results in acquiring critical awareness of potential security breaches or attempts made to gain unauthorized access. Through regular monitoring and logging of database activities, companies would be capable of detecting and responding to potential threats in real time. An instance of this activity in a database system is to use event logging through which any suspicious activities are logged in a secure and centralized location. This process helps the company in investigating and analyzing the logs to determine the potential security breaches and review the attempts made by unauthorized parties to gain access to the data.

7) Data Backups and Recovery

Data loss or system failure can be hindered by taking backups regularly. Every organization needs to establish an inclusive backup strategy to ensure that critical data is consistently backed up. For example, this can be done by implementing automated backup routines through which data are backed up on a daily or weekly basis in separate locations. It helps to restore the data when they get lost or corrupted, which causes business operations to be subject to minimum potential disruptions. In addition, backup and recovery can be considered a proper strategy against system failures and security breaches. Companies are required to define well-established processes to recover their data and systems so that downtime can be minimized and normal business operations can be restored. Data backup and recovery of a database system can be performed using automated recovery scripts or tools. This helps users quickly restore data and systems from backups and have minimum downtime and disruption rates for their business operations.

8) Incident Response Plans

These plans help manage and give suitable responses to security breaches or incidents that may occur in a database system. Companies need well-defined incident response procedures, such as communication plans, roles and responsibilities, and mitigation measures. An example of these plans in a database system is to activate a defined incident response team that can investigate and respond to security breaches or incidents. The team will be also capable of coordinating with IT and security teams, making effective communication with affected stakeholders, and taking appropriate mitigation measures into action.

9) Forensic Readiness

This refers to the ability to collect and preserve evidence concerning security breaches or incidents in database systems. It involves taking appropriate measures to preserve forensic artifacts, namely system configurations, log files, and network traffic, and being able to analyze and interpret this evidence, which is collected throughout forensic investigations. Forensic readiness in a database system is exemplified by using forensically sound software/hardware to acquire and preserve forensic evidence. Companies must have well-trained personnel in forensic analysis techniques that can competently assist them in the analysis and interpretation of forensic evidence.

10)Education and Awareness

For sensitive data to be well protected, employees need to be well-trained in database security and understand its importance. To reduce the risks of data breach, companies should take the most appropriate practices, find and mitigate potential risks, and enable their employees to resist them. This helps sensitive information to be kept with high confidentiality and integrity.

The DFRF's securing data storage system consists of 10 components working together to build a holistic view of the way sensitive data are protected. Organizations can create a strong security posture through the following practices: risk assessments, data classification, data encryption, implementation of database firewall, enforcement of strong password policies, monitoring, logging, backup administration, data recovery, and creation of a response plan when an incident occurs.

D. DFRF Validation

During this step, the developed framework was validated against the validation models identified in the previous step. Table IV provides a summary of the validation process. The results obtained disclosed that the developed DFRF model is comprehensive and covers most of the security components used in the database security and investigation domain.

TABLE II. VALIDATION PROCESS

Components involved in DFRF	**Validation models**							
	[6]	**[7]**	**[13]**	**[20]**	**[22]**	**[28]**	**[36]**	**[48]**
Risk assessment	√	√	×	√	×	×	×	×
Data classification	×	√	×	×	×	×	×	×
Data encryption	√	×	√	×	×	√	√	√
Database firewalls	×	×	×	×	×	√	×	×
Strong password policies	×	×	×	×	×	×	×	×
Database monitoring and logging	√	√	√	√	×	×	√	×
Data backups and recovery	×	×	√	×	×	×	×	×
Incident response plans	×	×	√	×	×	×	×	×
Forensic readiness	×	×	×	×	×	×	×	×
Education and awareness	×	×	×	×	×	×	×	×

IV. RESULTS AND DISCUSSION

A total of 57 models were collected and filtered. The review revealed that only one study [33] had covered the perspective of forensic readiness for database systems. The model proposed in [33] consists of three phases: pre-incident, during incident, and post-incident. However, it lacks some major forensic readiness components, such as risk assessment, strong password policies, and education and awareness. In addition, other models represented different investigation processes, as shown in Figure 7. Forensic readiness was covered only once, while the identification process was covered by 21 models and 19 models focused on collection and preservation. The analysis and examination process were covered by 47 models, while presentation and documentation were covered by 10 models. Therefore, most of the studies covered the analysis and examination process, followed by collection and preservation. It can be concluded that database systems still do not receive sufficient attention from researchers working in the field of digital forensics. This could be due to the heterogeneity and complexity of the architectures of database systems.

During this study, DSRM was utilized to develop DFRF, and the models were divided into two main categories: one for design and development and the other for validation. Figure 8 categorizes the development and validation models. Classifying the models into development and validation categories allows for a systematic approach to model development and validation. The development category encompasses 11 models that were initially identified, selected, and adapted for development. These models undergo a detailed development process that includes requirement gathering, combining, and harmonizing the investigation processes. The primary objective of the development category is to ensure that the model meets the desired specifications and delivers the functionality requested.

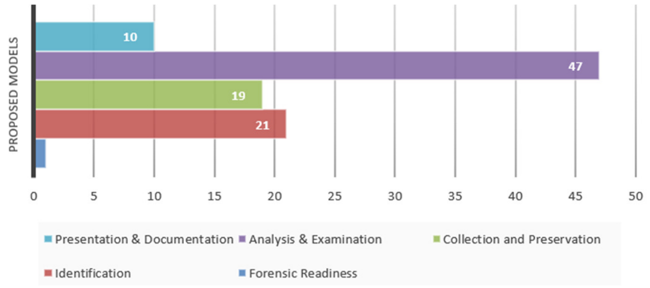

Fig. 7. Digital forensics models covering different investigation processes.

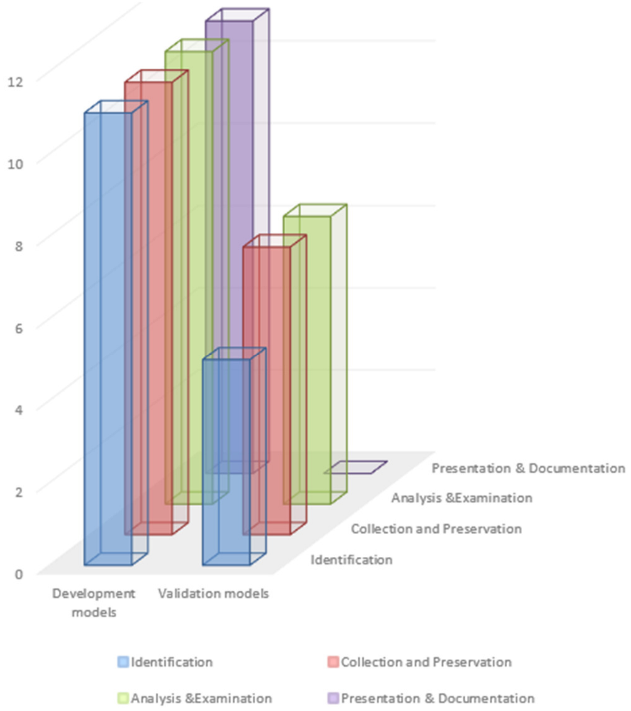

Fig. 8. Categorization of the development and validation models.

However, the validation category focuses on the assessment of the accuracy and reliability of the models developed. In this study, eight models were selected to validate the robustness, accuracy, and suitability of the proposed DFRF. Validation involves statistical analysis, empirical testing, or other validation techniques that can be used to ensure the effectiveness of a model's performance. This study proposed DFRF that combines all proactive components used in other previously proposed models to secure database systems. A key objective of the DFRF is to address the challenges that can be faced in the procedure of securing digital databases. It also helps to identify and respond proactively to potential security threats and attacks launched against data. Furthermore, DFRF contributes to the data security domain by helping organizations find and mitigate weaknesses in database systems. DFRF conducts routine audits and evaluations, which could result in the identification of possible weaknesses in system configuration, encryption measures, and access controls. Organizations can significantly reduce the risk of data breaches and improve the security of their databases by effectively dealing with these weaknesses.

V. CONCLUSION

Database systems perform different tasks, including structuring, organizing, and managing data. The integrity, confidentiality, and accessibility of an organization's database system could be compromised by many threats launched within and outside the organization. Parallel to the increase in the sophistication of attackers, security measures for database protection are continuously improved. In this sense, researchers and practitioners have proposed many traditional safety measures, such as data encryption, access control, database backups, database monitoring, and strong passwords. However, there are many challenges to the effectiveness of such security measures, including a lack of user awareness, insufficient data encryption, weak passwords, and limited capacity to detect and respond to database security threats. This study designed a digital forensic readiness framework, called DFRF, to secure database systems. This framework consists of 10 components: risk assessment, data classification, data encryption, database firewalls, strong password policies, database monitoring and logging, data backup and recovery incident response plans, and forensic readiness education and awareness. DFRF could help organizations improve their security postures, detect and provide appropriate responses to incidents, and fully comply with regulatory requirements. DFRF, compared to existing databases, offers a comprehensive approach to digital forensics. Future research should evaluate the performance quality of the developed DFRF in real-world scenarios.

REFERENCES

[1] M. Alam and K. A. Shakil, "Cloud Database Management System Architecture," *UACEE International Journal of Computer Science and its Applications*, vol. 3, no. 1, pp. 27–31.

[2] A. Alshammari, "A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11445–11450, Aug. 2023, https://doi.org/10.48084/etasr.6091.

[3] M. Ngadi, R. Al-Dhaqm, and A. Mohammed, "Detection and prevention of malicious activities on RDBMS relational database management systems," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, Sep. 2012.

[4] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, https://doi.org/10.48084/etasr.6195.

[5] 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.

[6] R. Susaimanickam, "A workflow to support forensic database analysis - Murdoch University," MSc Thesis, Murdoch University, Australia, 2012.

[7] H. Q. Beyers, "Database forensics : Investigating compromised database management systems," MSc Thesis, University of Pretoria, South Africa, 2013.

[8] A. Al-Dhaqm, S. Abd Razak, S. H. Othman, A. Nagdi, and A. Ali, "A Generic Database Forensic Investigation Process Model," *Jurnal Teknologi*, vol. 78, no. 6–11, Jun. 2016, https://doi.org/10.11113/jt.v78.9190.

[9] O. M. Fasan and M. Olivier, "Reconstruction in Database Forensics," in *Advances in Digital Forensics VIII*, Pretoria, South Africa, 2012, pp. 273–287, https://doi.org/10.1007/978-3-642-33962-2_19.

[10] O. M. Fasan and M. S. Olivier, "On Dimensions of Reconstruction in Database Forensics," in Proceedings of the Seventh International

Workshop on Digital Forensics and Incident Analysis (WDFIA 2012), 2012.

[11] I. S. Alansari, "A Detection and Investigation Model for the Capture and Analysis of Network Crimes," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11871–11877, Oct. 2023, https://doi.org/10.48084/etasr.6316.

[12] J. Yoon, D. Jeong, C. Kang, and S. Lee, "Forensic investigation framework for the document store NoSQL DBMS: MongoDB as a case study," *Digital Investigation*, vol. 17, pp. 53–65, Jun. 2016, https://doi.org/10.1016/j.diin.2016.03.003.

[13] D. Wong and K. Edwards, "System and method for investigating a data operation performed on a database," US20050289187A1, Dec. 29, 2005.

[14] H. K. Khanuja and D. S. Adane, "A framework for database forensic analysis," *Computer Science & Engineering: An International Journal*, vol. 2, no. 3, pp. 27–41, 2012.

[15] D. Litchfield, "Oracle Forensics - Part 1: Dissecting the Redo Logs," NGSSoftware Insight Security Research (NISR), Mar. 2007.

[16] D. Litchfield, "Oracle Forensics Part 2: Locating Dropped Objects," NGSSoftware Insight Security Research (NISR), Mar. 2007.

[17] D. Litchfield, "Oracle Forensics - Part 3: Isolating evidence of attacks against the authentication mechanism," NGSSoftware Insight Security Research (NISR), Mar. 2007.

[18] D. Litchfield, "Oracle Forensics Part 4: Live Response," NGSSoftware Insight Security Research (NISR), Apr. 2007.

[19] K. Fowler, *SQL Server Forenisc Analysis*. Pearson Education, 2008.

[20] N. Son, K. Lee, S. Jeon, H. Chung, S. Lee, and C. Lee, "The Method of Database Server Detection and Investigation in the Enterprise Environment," in *Secure and Trust Computing, Data Management and Applications*, Loutraki, Greece, 2011, pp. 164–171, https://doi.org/10.1007/978-3-642-22339-6_20.

[21] P. Frühwirt, M. Huber, M. Mulazzani, and E. R. Weippl, "InnoDB Database Forensics," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Perth, WA, Australia, Apr. 2010, pp. 1028–1036, https://doi.org/10.1109/AINA.2010.152.

[22] P. Frühwirt, P. Kieseberg, S. Schrittwieser, M. Huber, and E. Weippl, "InnoDB Database Forensics: Reconstructing Data Manipulation Queries from Redo Logs," in *2012 Seventh International Conference on Availability, Reliability and Security*, Prague, Czech Republic, Aug. 2012, pp. 625–633, https://doi.org/10.1109/ARES.2012.50.

[23] P. Frühwirt, P. Kieseberg, S. Schrittwieser, M. Huber, and E. Weippl, "InnoDB database forensics: Enhanced reconstruction of data manipulation queries from redo logs," *Information Security Technical Report*, vol. 17, no. 4, pp. 227–238, May 2013, https://doi.org/10.1016/j.istr.2013.02.003.

[24] G. T. Lee, S. Lee, E. Tsomko, and S. Lee, "Discovering Methodology and Scenario to Detect Covert Database System," in *Future Generation Communication and Networking (FGCN 2007)*, Jeju, Korea (South), Sep. 2007, vol. 2, pp. 130–135, https://doi.org/10.1109/FGCN.2007.106.

[25] J. Azemovi, "Efficient Model for Detection Data and Data Scheme Tempering with Purpose of Valid Forensic Analysis," presented at the International Conference on Computer Engineering and Applications, Singapore, 2011.

[26] R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper detection in audit logs," in *Proceedings of the Thirtieth international conference on Very large data bases*, Vol. 30, 2004, pp. 504–515.

[27] H. Khanuja and S. S. Suratkar, ""Role of metadata in forensic analysis of database attacks"," in *2014 IEEE International Advance Computing Conference (IACC)*, Gurgaon, India, Feb. 2014, pp. 457–462, https://doi.org/10.1109/IAdCC.2014.6779367.

[28] P. Frühwirt, P. Kieseberg, K. Krombholz, and E. Weippl, "Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations," *Digital Investigation*, vol. 11, no. 4, pp. 336–348, Dec. 2014, https://doi.org/10.1016/j.diin.2014.09.003.

[29] J. Yoon and S. Lee, "A method and tool to recover data deleted from a MongoDB," *Digital Investigation*, vol. 24, pp. 106–120, Mar. 2018, https://doi.org/10.1016/j.diin.2017.11.001.

[30] D. Litchfield, "Oracle Forensics Part 5: Finding Evidence of Data Theft in the Absence of Auditing," NGSSoftware Insight Security Research (NISR), Aug. 2007.

[31] D. Litchfield, "Oracle Forensics Part 6: Examining Undo Segments, Flashback and the Oracle Recycle Bin," NGSSoftware Insight Security Research (NISR), Aug. 2007.

[32] D. Litchfield, "Oracle Forensics Part 7: Using the Oracle System Change Number in Forensic Investigations," NGSSoftware Insight Security Research (NISR), Nov. 2008.

[33] 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.

[34] P. M. Wright, "Oracle Database Forensics using LogMiner," SANS Institute, Jun. 2004.

[35] A. Basu, "Forensic Tamper Detection in SQL Server." http://amitfrombangalore.blogspot.com/2015/08/forensic-tamper-detection-in-sql-server.html.

[36] M. J. Malmgren, "An Infrastructure for Database Tamper Detection and Forensic Analysis," BSc Thesis, University of Arizona, 2007.

[37] K. E. Pavlou and R. T. Snodgrass, "Forensic analysis of database tampering," *ACM Transactions on Database Systems*, vol. 33, no. 4, Sep. 2008, https://doi.org/10.1145/1412331.1412342.

[38] M. S. Olivier, "On metadata context in Database Forensics," *Digital Investigation*, vol. 5, no. 3, pp. 115–123, Mar. 2009, https://doi.org/10.1016/j.diin.2008.10.001.

[39] D. Lee, J. Choi, and S. Lee, "Database forensic investigation based on table relationship analysis techniques: 2009 2nd International Conference on Computer Science and Its Applications, CSA 2009," in *Proceedings of the 2009 2nd International Conference on Computer Science and Its Applications*, 2009, https://doi.org/10.1109/CSA.2009.5404235.

[40] F. Fatima, “Detecting database attacks using computer forensics tools,” Texas A&M University-Corpus Christi, 2011.

[41] H. Beyers, M. Olivier, and G. Hancke, "Assembling Metadata for Database Forensics," in *Advances in Digital Forensics VII*, Orlando, FL, USA, 2011, pp. 89–99, https://doi.org/10.1007/978-3-642-24212-0_7.

[42] H. Beyers and M. Olivier, "An Approach to Examine the Metadata and Data of a Database Management System by making use of a Forensic Comparison Tool," 2011.

[43] S. Tripathi and B. B. Meshram, "Digital Evidence for Database Tamper Detection," vol. 2012, Apr. 2012, https://doi.org/10.4236/jis.2012.32014.

[44] S. Jeon, J. Bang, K. Byun, and S. Lee, "A recovery method of deleted record for SQLite database," *Personal and Ubiquitous Computing*, vol. 16, no. 6, pp. 707–715, Aug. 2012, https://doi.org/10.1007/s00779-011-0428-7.

[45] P. D. Abhonkar and A. Kanthe, "Enriching forensic analysis process for tampered data in database," *International Journal of Computer Science and Information Technologies*, vol. 3, no. 5, pp. 5078–5085, 2012.

[46] H. Q. Beyers, M. S. Olivier, and G. P. Hancke, "Arguments and Methods for Database Data Model Forensics," in *Proceedings of the Seventh International Workshop on Digital Forensics and Incident Analysis (WDFIA 2012)*, 2012.

[47] H. K. Khanuja and Dr. D. S. Adane, "Forensic Analysis of Databases by Combining Multiple Evidences," *International Journal of Computers and Technology*, vol. 7, no. 3, pp. 654–663, Jun. 2013, https://doi.org/10.24297/ijct.v7i3.3446.

[48] K. E. Pavlou and R. T. Snodgrass, "Generalizing database forensics," *ACM Transactions on Database Systems*, vol. 38, no. 2, Apr. 2013, https://doi.org/10.1145/2487259.2487264.

[49] O. M. Adedayo and M. S. Olivier, "On the Completeness of Reconstructed Data for Database Forensics," in *Digital Forensics and*

Cyber Crime, Lafayette, IN, USA, 2013, pp. 220–238, https://doi.org/10.1007/978-3-642-39891-9_14.

[50] P. P. Gawali, "Forensic Analysis Algorithm: By using the Tiled Bitmap with Audit Log Mechanism," *International Journal of Computer Applications*, vol. 63, no. 11, pp. 36–42, Feb. 2013.

[51] B. Wu, M. Xu, H. Zhang, J. Xu, Y. Ren, and N. Zheng, "A Recovery Approach for SQLite History Recorders from YAFFS2," in *Information and Communication Technology*, Yogyakarta, Indonesia, 2013, pp. 295–299, https://doi.org/10.1007/978-3-642-36818-9_30.

[52] J. H. Choi, D. W. Jeong, and S. Lee, "The method of recovery for deleted record in Oracle Database," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 23, no. 5, pp. 947–955, 2013, https://doi.org/10.13089/JKIISC.2013.23.5.947.

[53] M. Xu *et al.*, "A metadata-based method for recovering files and file traces from YAFFS2," *Digital Investigation*, vol. 10, no. 1, pp. 62–72, Jun. 2013, https://doi.org/10.1016/j.diin.2013.02.006.

[54] P. P. Gawali, "Database tampering and detection of data fraud by using the forensic scrutiny technique," *International Journal of Emerging Technology and Advanced Engineering3*, vol. 3, no. 2, pp. 439–446, Feb. 2013.

[55] M. Xu *et al.*, "A Reconstructing Android User Behavior Approach based on YAFFS2 and SQLite.," *Journal of Computers*, vol. 9, no. 10, pp. 2294–2302, 2014.

[56] W. K. Hauger and M. S. Olivier, "The role of triggers in database forensics," in *2014 Information Security for South Africa*, Johannesburg, South Africa, Dec. 2014, pp. 1–7, https://doi.org/10.1109/ISSA.2014.6950506.

[57] H. K. Khanuja and D. S. Adane, "Forensic Analysis for Monitoring Database Transactions," in *Security in Computing and Communications*, Delhi, India, 2014, pp. 201–210, https://doi.org/10.1007/978-3-662-44966-0_19.

[58] O. M. Adedayo, "Reconstruction in Database Forensics," Ph.D. dissertation, University of Pretoria, South Africa, 2015.

[59] J. Wagner, A. Rasin, and J. Grier, "Database forensic analysis through internal structure carving," *Digital Investigation*, vol. 14, pp. S106–S115, Aug. 2015, https://doi.org/10.1016/j.diin.2015.05.013.

[60] O. M. Adedayo and M. S. Olivier, "Ideal log setting for database forensics reconstruction," *Digital Investigation*, vol. 12, pp. 27–40, Mar. 2015, https://doi.org/10.1016/j.diin.2014.12.002.

[61] J. O. Ogutu, "A Methodology To Test The Richness Of Forensic Evidence Of Database Storage Engine: Analysis Of MySQL Update Operation In InnoDB And MyISAM Storage Engines," MSc Thesis, University of Nairobi, Kenya, 2016.

[62] 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, Feb. 2016, https://doi.org/10.19026/rjaset.12.2377.

[63] J. Wagner, A. Rasin, T. Malik, K. Heart, H. Jehle, and J. Grier, "Database Forensic Analysis with DBCarver," in *CIDR 2017, 8th Biennial Conference on Innovative Data Systems Research*, Jan. 2017.

[64] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," *PLOS ONE*, vol. 12, no. 2, 2017, Art. no. e0170793, https://doi.org/10.1371/journal.pone.0170793.

[65] M. Alam and K. A. Shakil, "Cloud Database Management System Architecture," *UACEE International Journal of Computer Science and its Applications*, vol. 3, no. 1, pp. 27–31, https://doi.org/10.1109/ACCESS.2017.2762693.

[66] 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, Nov. 2018, pp. 75–80, https://doi.org/10.1109/AINS.2018.8631468.

[67] R. Bria, A. Retnowardhani, and D. N. Utama, "Five Stages of Database Forensic Analysis: A Systematic Literature Review," in *2018 International Conference on Information Management and Technology (ICIMTech)*, Jakarta, Indonesia, Sep. 2018, pp. 246–250, https://doi.org/10.1109/ICIMTech.2018.8528177.

[68] 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.

[69] H. Choi, S. Lee, and D. Jeong, "Forensic Recovery of SQL Server Database: Practical Approach," *IEEE Access*, vol. 9, pp. 14564–14575, 2021, https://doi.org/10.1109/ACCESS.2021.3052505.

[70] M. F. Caro, D. P. Josyula, M. T. Cox, and J. A. Jiménez, "Design and validation of a metamodel for metacognition support in artificial intelligent systems," *Biologically Inspired Cognitive Architectures*, vol. 9, pp. 82–104, Jul. 2014, https://doi.org/10.1016/j.bica.2014.07.002.

[71] S. Kelly and R. Pohjonen, "Worst Practices for Domain-Specific Modeling," *IEEE Software*, vol. 26, no. 4, pp. 22–29, Jun. 2009, https://doi.org/10.1109/MS.2009.109.