IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 21, 2020, accepted July 6, 2020, date of publication July 13, 2020, date of current version August 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3008696

Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field

ARAFAT AL-DHAQM[1,2], (Member, IEEE), SHUKOR ABD RAZAK[1], (Member, IEEE), KAMRAN SIDDIQUE[3], (Member, IEEE), RICHARD ADEYEMI IKUESAN[4], AND VICTOR R. KEBANDE[5]

[1]Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia (UTM), Skudai 81310, Malaysia
[2]Department of Computer Science, Aden Community College, Aden, Yemen
[3]Information and Communication Department, School of Electrical and Computer Engineering, Xiamen University Malaysia, Sepang 43900, Malaysia
[4]Department of Cybersecurity and Networking, School of Information Technology, Community College of Qatar, Doha, Qatar
[5]Computer Science and Media Technology Department, Malmö Universitet, 211 18 Malmö, Sweden

Corresponding authors: Arafat Al-Dhaqm (mrarafat@utm.my) and Kamran Siddique (kamran.siddique@xmu.edu.my)

This work was supported in part by the Research Management Center, University Technology Malaysia through the Modeling Information Security Policy Field, under Grant R. J130000.7113.04E96, and in part by the Research Management Center, Xiamen University Malaysia through the Xiamen University Malaysia Research Program Cycle Three, under Grant XMUMRF/2019-C3/IECE/0006.

ABSTRACT For every contact that is made in a database, a digital trace will potentially be left and most of the database breaches are mostly aimed at defeating the major security goals (Confidentiality, Integrity, and Authenticity) of data that reside in the database. In order to prove/refute a fact during litigation, it is important to identify suitable investigation techniques that can be used to link a potential incident/suspect to the digital crime. As a result, this paper has proposed suitable steps of constructing and Integrated Incident Response Model (IIRM) that can be relied upon in the database forensic investigation field. While developing the IIRM, design science methodology has been adapted and the outcome of this study has shown significant and promising approaches that could be leveraged by digital forensic experts, legal practitioners and law enforcement agencies. This is owing to the fact, that IIRM construction has followed incident investigation principles that are stipulated in ISO guidelines.

INDEX TERMS Database security, database forensics investigation, database incident, pre-incident response, during-incident response, post-incident response.

I. INTRODUCTION

It is needful for organizations to protect their assets, capitals, employees' information, current and future projects, strategies, and plans in their database systems from potential intrusions or attacks. Notably, insider and outsider attacks are often considered as a high priority especially to the top management of any organization especially when they jeorpardize the security goals-Confidentiality, Integrity, and Availability (CIA) triad of database systems. We, therefore, posit that security models are essential for operational and business continuity purposes for all organizations. However, the core of such operation in the current technology-driven environment, is hinged on having a secure database system. Based on the existing literature, numerous database security models have been developed before to protect database systems, with diverse representations which have led to the diversification as far as security formalism in the database discipline is concerned. However, these models vary in many aspects as they tend to deal with different issues of database security [1]. Consequently, they may also differ because they provide varying assertions and different paradigms which have different meanings on what constitutes a secure database. Also, a lack of knowledge that is needed to fulfill security models, controls, enforce policies, or conduct incident response processes [2] has induced the basis for the diversity of the security periscope among these studies. These, among other ambiguities and disparities have further complicated the security layers for database researchers. One approach that can be used to address these ambiguities, as revealed

The associate editor coordinating the review of this manuscript and approving it for publication was Gianmaria Silvello.

in other disciplines, is the development of a standardized or harmonized investigative framework for database forensics. Whilst there exist samples of harmonized models for the general body of digital forensics, the scope of database forensics is least explored at the time of writing this paper. Unlike other forensic disciplines, database forensics provides the base from which most forensic disciplines operate. Sadly, attention has not been geared towards developing formalized approaches/processes that can act as a foundation for database forensics. A formal integrated investigation framework would, therefore, require the development of each component of a typical forensic process model (potential evidence identification, collection, extraction, storage, analysis, documentation and presentation, and business continuity), albeit, for database forensics. For instance, the ISO/IEC 27043: 2015 [3] and several related frameworks for incidents response has been identified in cloud forensics [4], malware forensics [5], [6], Software-Defined Networks (SDN) [7], as well as in computer forensics [8], [9]. As a step in this direction, this study explored the potential of developing a representative reference model for handing incidents in typical database forensics. As highlighted in the study in [10], a robust Integrated Incident Response Model (IIRM) to recognize, respond, mitigate, and resume the database incidents is critically essential for the development of the database forensic discipline.

Thus, this study proposes an IIRM to recognize, respond, mitigate, and recover from a potential database incident. The proposed IIRM, therefore, answers the following questions:

1. What incident response strategy should be taken before, during, and after incident identification?
2. What kinds of information security policies should be applied during incident-response?
3. What immediate actions should be taken (e.g., should the database server be unplugged from the network)?
4. Who should be notified and in what order?
5. How should volatile data be handled?
6. How can potential digital evidence be gathered and preserved in a forensically sound manner (e.g., should the computer be left ON to preserve the potential digital evidence in memory)?
7. How can the affected database system be restored and recovered?

To achieve the main objective in this paper, we adapt the design science research method towards the development of the IIRM. The developed IIRM consists of three processes namely: i) Pre-incident response stage, ii) During-incident response stage, and iii) Post-incident response stage. More subprocesses in the IIRM will become apparent in the later sections of this paper.

The rest of the manuscript is organized as follows: Section 2 offers the study background and related works. Section 3 provides the methodology. Section 4 provides discussion and analysis results. Section 5 concludes this paper and mentions future work.

II. BACKGROUND AND RELATED WORKS

This section gives relevant research that has somewhat been used as background and related work. The concertation has been on the literature on databases and database forensics in general.

Based on existing literature, several incident-related models have been developed bas for database forensic investigations. These models typically comprise of components that primarily are inclined to the following: approaches to identify, collect, preserve, reconstruct, analyze, and document pieces of evidence, or potential pieces of evidence against database incidents [11]. In this regard, an integrated model was proposed by the study in [12], which deals with database incidents from three perspectives: *preparation and response*, *acquisition and preservation*, and *analysis and reconstruction*. More detailed explanations of these perspectives have been explained further on.

A. PREPARATION AND RESPONSE (PERSPECTIVE I)

The first perspective of that model examines database incident models from a preparatory and response view. However, the suspension of the database process [12] separates the database server from the clients to obtain database actions, while the authentication and system description processes [13] verify database incidents, separates the database server, prove the incident, and documents the system information. Besides, the identification process [14] deals with isolating database server from the network to obtain volatile-data. Similarly, the incident verification process and investigation preparation process [15] is used to detect and validate database incidents through an initial examination, prepare forensic toolkits, and forensic environment to reply to occurrences and then isolate the database server. Furthermore, the database connection environment process [16] prepares the examination environment and to gain the required authorization needed to gain access to the database to fulfill necessary instructions. Additionally, the purpose of the join and table relationship search process is to obtain tablespaces in the database, choose the goal, choose the tables that store inspection data, and frequently examine the other table field. A search warrant and data acquirement with the seizure process need capturing the place of sign and obtaining evidence that connects to an incident [17]. Next, the server detection process [18] is used to identify and detect the victim database server and acquiring the network topology inside the company. The setup evidence collection server process [19] is applied to organize the examination environment to warehouse incidents, while the identification process [20] detects related MySQL database files (text files, log files, binary files) and services. Incorporated is also the incident reporting and examination preparation processes [21] that are utilized to obtain database incidents via user reports. Researchers in [22] suggested determining database dimension and acquisition processes, which are utilized for discovering which dimension of the database has been damaged or attacked.

The chosen environment and the selected implementation methods and processes [23] are used to select the forensic environment (clean or found environment), select a method that used to transform the forensic setting into the selected forensic environment. The preliminary analysis process [24] is aimed to create an architectural visualization of the DBMS with all the components and their location within the layered model of DBMS.

B. ACQUISITION AND PRESERVATION (PERSPECTIVE II)

The second perspective inspected database incident models from acquisition and preservation view. For example, the data gathering process [25] is aimed at collecting data, and attacked events. It also explored the evidence collection process which is used to collect data from the victim database server, and an evidence collection process [13] to gather volatile data from victim database servers. The artifact collection process [14] is aimed at gathering volatile and non-volatile MSSQL Server database artifacts such as log files, data files, a data cache, transaction logs, and log files. The data extraction process proposed by [16] is used to extract data on relationships that connect columns in database tables. Also, the beginning of the investigation process proposed by [17] has similar activities designed to extract fraud data from a database server. The metadata extraction process proposed by [18] is used to extract the metadata of the database dimension and determine who was authorized to perform a certain action. The data collection process presented by [18] is subdivided into two stages that consist of a stage dedicated to selectively files and another stage that focuses on collecting entire files. Moreover, the file collection process was proposed by [19] to collect Oracle files from specific locations and move them to the evidence collection server for further investigation. The artifact collection process was also proposed by [20] to collect and extract database files and metadata from compromised MySQL Server databases. Similarly, [14] proposed a *collection process* as a sub-process of physical and digital examination to collect physical and digital data. The collection of volatile artifacts and non-volatile artifacts processes were proposed by [15] to collect database files, log files, log transactions, and also volatile artifacts such as data caches, redo log, and undo log. This is similar to the artifact collection process proposed by [16], and artifact collection process proposed by [20]. The collection process of the database system proposed by [16] allows investigators to collect and extract suspected database management system data and move it to a secure area for further forensic investigation. Furthermore, the collection, and preservation process proposed by [24] allows investigators to collect detailed multiple logs of SQL, MySQL, and operating systems. Similarly, the collection process proposed by [26] gathers evidence from replicating sources. Finally, the execution process proposed by [28] allows investigators to use forensic tools and procedures to create forensic values and then collect metadata values of the identified target files.

C. RECONSTRUCTION (PERSPECTIVE III)

The third perspective reviewed database incident models from analysis and reconstruction view. For example, two processes have been proposed by [12] to reconstruct and restore database systems: reconstructing a database and restoring database integrity. The reconstruction of a database is used to rebuild intruder activities and reveal malicious actions, while the restoring database integrity is used to restore database consistency. Four investigation processes have been proposed by [13] to analyze database crimes: timeline creation, media analysis, data recovery, and string search. The timeline creation process is used to construct an initial timeline that maps out notable digital events that will be used during the Media Analysis process. The media analysis process uses the timeline of events constructed in the timeline creation process to reveal malicious intruder activities. After discovering malicious activities, the database system needs to recover data to be ready for user access through the data recovery process. The search string process was used to further investigate transactions that occurred outside of the scope of this investigation to identify rows for reconstruction.

III. PROBLEM STATEMENT

Based on the literature review that has been discussed in Section II, it has become apparent that numerous database incident-based models have been developed to identify, collect, preserve, reconstruct, analyze and document pieces of evidence against database incidents, however, these models vary in many phases, procedures, and activities as they deal with different issues of database incidents. Furthermore, they differ also because they present divergent assertions on what represents a secure database. Thus, existing research works have not concentrated on addressing fundamental and essential guidelines that can be useful for establishing a baseline for database incidents. Rather, these researches have mainly focused on specific procedures and principles of technical issues that address specific problems. Therefore, there is a lack of a structured and unified incident response model that can satisfy the needs, report, or data exchange that is important to the domain practitioners in the forensic community. Besides, existing models largely ignored the forensic soundness of any potential evidence that may be identified to corroborate investigative claims.

IV. METHODOLOGY

In this section, we will explain the criteria used in the design science method which is useful in solving a problem that has been unsolved before or solving a known problem more effectively or efficiently. According to the assertion in [29], the design science method is a methodology that is suitable for developing a model that contributes to the growth of knowledge in the domain. Consequently, the design science method has been defined in Othman's study [30] which is further modified as shown in Fig 1., presents a suitable method for this purpose. Therefore, the adapted method shown in Fig 1. is used to develop the concepts and the

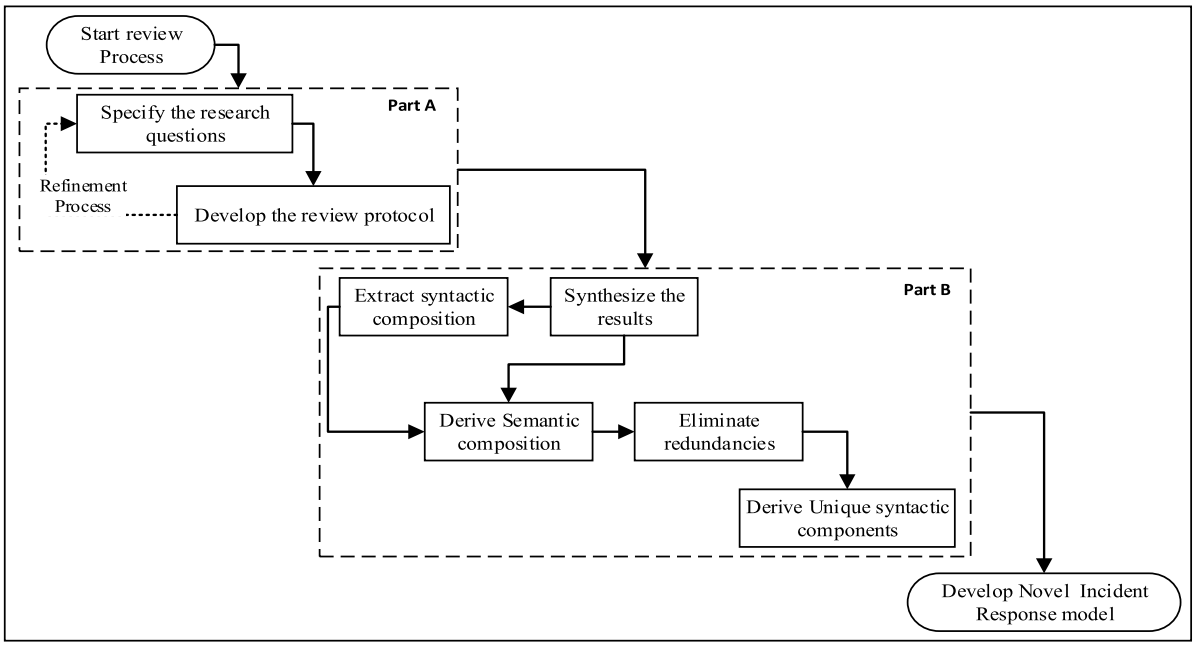

FIGURE 1. Adapted framework for the model development process.

overall model of this study. The methodology comprises two composite functionalities (Part A & Part B). To begin the integrated model development process, the study attempted to formulate specific research questions which center on the degree of availability of incident response research. A preliminary investigation of the research questions revealed several classes of terminologies with similar (or identical in some cases) conceptual definition or meaning, albeit, used as a distinct phase of the investigation process (in several research manuscripts from scientific repositories). The scientific repositories considered in this study include IEEE Xplore, Scopus, ACM, SpringerLink, and Elsevier. They were selected based on the available institutional subscription, and a general computer science scope. To provide a finer clarity of each concept, a review protocol was developed. However, this process follows an iterative approach, such that a steady refining of the review protocol was carried until no related literature was observed in the selected repository (a process often referred to saturation of the search space). The output of these processes is then fed into the next composite process, ***Part B***, as highlighted in Fig 1. This process leverages the principle of semantic similarity among candidate concepts. It involves the extraction of syntactic and semantic characteristics from each concept (in each identified model) and then, the elimination of redundancies among the models to generate unique components that can be used to develop an integrated model.

Supposed that the semantic composition of a syntactic composition (S_y) of a concept (C) is further denoted by the expression; $S_e = \forall S_y \in C, \exists S_y \in C_i \wedge C_j \Rightarrow \therefore S_e \ni \{S_y \in C_i\} \triangleq S_e \ni \{S_y \in C_j\}$ where C_i and C_j have been identified in existing studies as separate concepts. A new syntactic component can then be defined based on this semantic similarity/similarities. The eventual outcome of such a series of syntactic composition derivation can then be used to develop an integrated incident response model for DBFI which is void of redundancy. Elaboration of these processes is further provided in the subsequent subsections, labeled as Phases 1, 2, and 3.

Phase 1: Identify and Select Domain Models

In this step, the database forensic investigation models were identified and selected. Several models were discussed and analyzed in the literature review. Model selection for this study was based on coverage factors that were identified in previous research [11]. Wide coverage of database forensic investigation processes that are broadly applicable is required to fulfill the aim of categorizing the investigation process. Using a coverage metric quickly indicates sourced model applicability. The model is said to have a high coverage value if the model has at least two investigation processes. The model has a reduced amount of coverage value if the model only describes one database forensic investigation process. The output of this step is twenty-two (22) common models for categorization purposes as shown in Table 1.

Phase 2: Extract Relevant Processes

In this step investigation processes from the 22 models were extracted based on criteria adapted from [45], [46]:

i. Titles, abstracts, related works, and conclusions were excluded: the investigation process was either extracted from the diagram or the main textual model.
ii. The investigation process must have a definition, activity, or task; to recognize the purpose and meaning of the process.
iii. Irrelevant investigation processes not related to conducting DBFI were excluded.

TABLE 1. Identified and Selected Models.

ID	Year	Selected Models
1.	2004	System and method for investigating a data operation performed on a database [12]
2.	2005	Forensic Analysis of a SQL Server 2005 Database Server [13]
3.	2007	Oracle Forensics Live Response [14]
4.	2008	SQL Server Forensic Analysis Methodology [15]
5.	2009	Database forensic investigation based on table relationship analysis techniques [16]
6.	2009	Evidence Investigation Methodologies for Detecting Financial Fraud based on Forensic Accounting [17]
7.	2009	On metadata context in Database Forensics [11]
8.	2011	The Method of Database Server Detection and Investigation in the Enterprise Environment [18]
9.	2012	Digital Evidence for Database Tamper Detection [19]
10.	2012	Framework for Database Forensic Analysis [20]
11.	2012	A Workflow to Support Forensic Database Analysis [21]
12.	2012	On Dimensions of Reconstruction in database forensic [22]
13.	2013	Forensic Analysis of Databases by Combining Multiple Pieces of evidence [26]
14.	2014	Database Forensics: Investigating Compromised Database Management Systems [23]
15.	2014	Role of metadata in forensic analysis of database attacks [27]
16.	2014	Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations [28]
17.	2015	Ideal log setting for database forensics reconstruction [33]
18.	2015	Database forensic analysis through internal structure carving [34]
19.	2016	A Methodology to Test the Richness of Forensic Evidence of Database Storage Engine: Analysis of MySQL Update Operation in InnoDB and MyISAM Storage Engines [41]
20.	2016	A generic database forensic investigation process model [42].
21.	2018	CDBFIP: Common database forensic investigation processes for internet of things [43].
22.	2018	Five Stages of Database Forensic Analysis: A Systematic Literature Review [44]

iv. Include explicit and implicit investigation processes from models. As shown in Table 2 it was discovered there are twenty-one (21) processes from the 22 models. Most of these 21 processes are redundant and need to be merged and grouped into a specific categorization. The next section discusses this merging process.

Phase 3: Combined Similar Processes

The first categorization examined investigation processes from an incident response and preparation perspective. For example, the *Suspension of Database Operation* process in the model of [12] cuts off access to the database server for users to enable the capture of database activities, while the *Verification and System Description* processes in the model of Fowler [13] verifies and checks database incidents, isolates

TABLE 2. Extracted Processes.

No	Similar Processes	Activity and Meaning
1.	Suspend Database Operations	Database operations are suspended, at least long enough to capture evidence of the intruder's actions. This may entail disabling new logins, terminating any or all existing sessions, and disconnecting users from the database.
2.	Verification	Verifies and checks incident isolates database server and confirms the incident.
3.	System Description	Documents system information identified in the verification processes, i.e. system name, serial number, operating system, system function, and physical description.
4.	Identification process	Disconnects database server from network to capture volatile data as well as prepare forensic environment and forensic techniques used to move captured data.
5.	Identification process	Used to disconnect the database servers from the network to capture volatile data as well as prepare forensic environment and forensic techniques used to move captured data.
6.	Investigation Preparation	Identifies and prepares forensic workstations and forensic toolkits to respond to an incident and then disconnects from the database server.
7.	Incident Verification	Verifies the database incident through preliminary investigation.
8.	Database Connection Environment	Prepares the investigation environment and obtains the right to access the database and execute the command.
9.	Table Relationship Search and Join Process	Used to extract all table-spaces in the database, select the target, select the tables which store investigation data, and repeatedly check the other table field.
10.	Data Acquirement with Seizure and Search Warrant	Detect and secure database system resources and gather evidence that relates to accounting fraud. Protects the data resources of the corporation. Also, conduct an interview with DBA to validate the existence of a server managed by the corporation.
11.	Server Detection	Server detection is used to identify and detect the victim database server.
12.	Setup Evidence Collection Server	Preparing the investigation environment to reveal an incident.
13.	Incident reporting	capture database incident through user report, system audit, or triggered events
14.	Examination Preparation	Used to detect a database incident, isolate a network, configure an investigation environment, identify policies, and prepare proper forensic tools as well as making decisions about the next steps.
15.	Determine Database Dimension	Identifies which dimension of the database has been attacked or hacked
16.	Determining Acquisition Method	Identifies the proper acquisition methods for that dimension.
17.	Identification	Prepare the database forensic layers, methods and environment
18.	Preliminary analysis	Create an architectural visualization of the database, identify files and folders in layers below the storage engine layer, prepare and use forensic tools and procedures to create an initial image, collect and record metadata values of the identified target files.
19.	Identification	Used to prepare laws and regulations, investigation techniques, investigation team, policies, database resources, investigation environment

TABLE 2. ***(Continued.)*** **Extracted Processes.**

No	Similar Processes	Activity and Meaning
20.	Identification	Used to prepare a clean database forensic investigation environment and trusted forensic techniques; Allows the investigation team to isolate the database server from the network to prevent users from tampering with and capturing volatile and non-volatile data.
21.	Database Identification	Introduced to define, identify, prepare, detect, and investigate database incidents. This is the initial process of an investigation to find out a problem in the database. This can help to find the investigation methods to be used in the investigation.

the database server, confirms the incident, and documents system information such as system name, serial number, operating system, system function, and physical description. Also, the *Identification* process in [14] model provides for disconnecting the database server from the network to capture volatile data. Similarly, the *Investigation Preparation* and *Incident Verification* processes in [15] model are used to identify and verify database incidents, begin a preliminary investigation, prepare workstations and tools for incident response, and disconnect the database server.

Furthermore, the *Database Connection Environment* process in the model proposed by [16] prepares the investigation environment and obtains the necessary permissions to be able to access the database and execute the required commands. Also, the purpose of the *Table Relationship Search and Join* process is to extract table-spaces in the database, select the target, select the tables which store investigation data, and repeatedly check the other table field.

The *Data Acquirement with Seizure and Search Warrant* process requires securing the incident scene and extracting evidence that relates to a crime or an incident [17]. Another process is the *Server Detection* process used to detect any server hosting a database system. This process includes understanding the overall network inside a company; and acquiring the network's topology to identify and detect the victim database server [18]. The *Setup Evidence Collection Server* process described in the [32] model is used to prepare the environment to store recorded incidents, while the *Identification* process described in [20] identifies relevant database files (text files, log files, binary files) and utilities. Similarly, [21] proposed an *Incident Reporting and Examination Preparation* process, which is used to capture database incidents through user reports, system audits, and/or triggered events. Database incidents are then handled by cutting off the network, configuring the investigation environment, identifying violated policies, preparing the proper tools, and informing the decision-maker. Also, [22] suggested *Determining Database Dimension and Acquisition Method* processes, which are used for identifying which dimension of the database has been attacked or hacked. Once this has been achieved, the proper acquisition methods for that dimension are then identified. Also, the *Choose Environment and Select Implement Method* process proposed by [23] is used to select the forensic environment (clean or discovered environment) and select a method that is used to transform the forensic setting into the selected forensic environment. Also, the *Preliminary Analysis* process is proposed by [41] that aimed to create an architectural visualization of the database with all the components and their location within the layered model of the DBMS, identify files and folders in layers below the storage engines' layer, prepare and use forensic tools and procedures to create an initial image and then collect metadata values of the identified target files, and record the metadata of the target files. The *Identification* process is offered by [42] that intended to prepare laws and regulations, investigation techniques, investigation team, policies, database resources, investigation environment, authorization, detection server, interview, detection database incident, and incident report. Also, the *Identification* process proposed by [43] is used to prepare a clean database forensic investigation environment and trusted forensic techniques, as well as allow the investigation team to isolate the database server from the network to prevent users from tampering with it and to capture volatile and non-volatile data. Finally, [44] introduced a *Database Identification* process useful for defining, identifying, preparing, detecting, and investigating database incidents. This is the initial process of an investigation to find a problem in the database. This can help to identify the investigation methods to be used in this investigation process.

Thus, twenty-one (21) investigation processes have been organized and merged in the first category based on their similar activities or meaning as shown in Table 2.

A. PROPOSED COMMON PROCESSES

Implicitly, previous database incidents models have focused on one stage of database incidents response to reveal database incidents and that is the stage of incident response. However, the focus has not been on pre-incident response. Therefore, the model that has been proposed in this paper consists of three stages as follows: i) pre-incident response, during-incident response, and iii) post-incident response. Additionally, it is important to note that this proposed model leverages knowledge from the activities and procedures from existing literature into one common model termed as incident response model (IIRM). Each stage of the IIRM has several procedures and policies that react immediately and efficiently to mitigate the urgent damage to the DB, eliminate any possible consequential losses, and prevent any possible future repetition and a description of each follows.

High-Level Representation of Stages based on ISO/IEC 27043 concepts

Based on the aforementioned three stages(i) pre-incident response, during-incident response, and iii) post-incident response.), the authors of this paper have taken a high-level approach of fitting this study into harmonized investigative processes that give guidelines for representing high-level concepts in investigative processes as per the case of the proposed

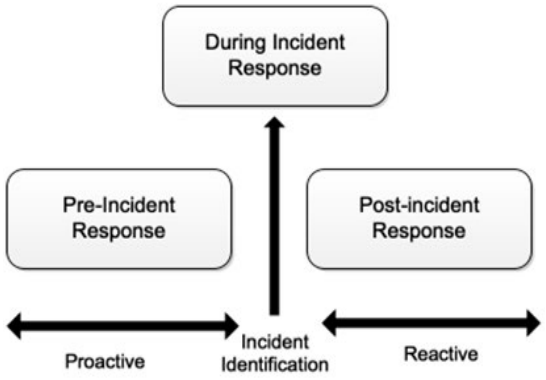

FIGURE 2. High-level representation of IIRM based on ISO 27043 guidelines.

IIRM model. It is the author's opinion that from these three stages, this study addresses the challenges of before and after-incident identification problem of the database forensic field. Therefore, the three stages have been mapped with ISO/IEC 27043: 2015 guidelines to ascertain where each stage (process) can fit or could be categorized. This is useful because it helps to identify the disparities that may exist when exploring investigation processes between the three different stages. That notwithstanding, it is imperative to have redundant processes during an investigation, and hence by categorizing the stages, it becomes easy to explicitly identify these redundancies based on the categorization. Fig 2. categorizes the process (stages) based three aspects: Proactive (Pre-incident response) Incident identification (During incident response) and Reactive (Post-incident Response). An explanation of how they fit into the ISO/IEC 27043 standard is given next.

Fig 2. shows how the IIRM translates and fits into the ISO/IEC 27043 guidelines on incidents. For example, Pre-incident response translates into planning and preparedness (Readiness process) which is a proactive forensic approach, while incident response translates to incident identification approach. Lastly, post-incident response translates and fits into the response process which is a reactive process. These are generally the applicative approaches to the investigative classes that allow preparing and responding during database forensic investigations.

This is an abstract representation that is useful in giving a generic view of the IIRM having in mind that the processes that have been used while constructing IIRM follow scientific digital forensic processes which later openly precludes repetition and redundancies by allowing the IIRM to be decomposed into other relevant processes. Having looked into how the IIRM fits into the standardized processes, an explanation of the three stages is expounded next.

Stage I: Pre-Incident Response

This stage translates into a security policy that acts as a readiness phase that prepares for potential database incidents. Security policies can be applied to control the execution of the requested actions on the database systems. The security policy should not merely identify the valid user rights, but also help in the discovery of the misuse of the rights and adjust to identify circumstances that can lead to threats in the system. Thus, a security policy is a specification of security requirements, usually specified based on some security model. Therefore, the security manager and DBA must prepare a security policy to prevent and protect the database systems from any malicious activities. A security policy should include the following:

a) *User Identification and Authentication*: Identified and verified client identity method is utilized to decide who wins admission to local properties. Logging of both failed and successful attempts should also be enabled.
b) *Enable Firewall*: A firewall considered the first defense line of security measures, which protects the network and database systems from insider and outsider attacks. The purpose of a firewall is to investigate each new or out packet and determine whether to recognize or reject it. This work is usually required by a series of guidelines. the efficiency of the rules, in terms of accuracy and reliability, should be logged. Therefore, the efficiency of the firewall concerning false/true positive/negative should be documented in a log file.
c) *Install Intrusion Detection and Prevention Systems (IDPSs):* The organization must install high developed IDPS that can be used to detect malicious activities. IDS is one of the crucial methods to accomplish high protection in computer networks and utilized to avoid various incidents. IDPSs inherently induce curse-of-dimensionality problems in a typical behavioral analysis challenge which manages to improve the time difficulty and reduce source consumption. As a result, feature optimization processes should be applied in the development of an intrusion detection system to reduce dimensionality. Similarly, logging of processes and actions must be enabled in the IDPS which is further fed into the audit engine.
d) *Enable Auditing and Accountability*: Auditing is the process of examining and making a recording of configured database activities, from all database users privilege notwithstanding. Accounting involves the act of keeping an audit track for all user activities on a given system. Both audit examinations and accountability are essential to ensure the physical integrity of the data source, and the logical integrity of the data. This process is often handled through the auditing of the system. It is also a requirement for keeping the records. If a user has been successfully authenticated and such a user attempts to gain access to a source, both effective and failed attempts are examined by the system. Furthermore, access tries, and the corresponding position should seem in the examination trail files. Therefore, it is essential to enable all audit logs to be able to re-create an event and trace the entire activities of a targeted user.
e) *Identify Sensitive Information*: Before the application of any cryptographic mechanism on the sensitive information, there will be a need to classify information

based on the degree of sensitivity. To this end, a process of identifying and classifying sensitive information should be deployed by the organization.

f) *Scheduling Full backup:* A full backup is a copy at a particular point in time of all the files to be backed up from the primary storage device. Thus, scheduling full backup of system configurations, and database systems are important to save the continuity of the business in case of failure happened. Therefore, the DBA must take at least one full-back once a week or a month. Then enable incremental backup. An incremental backup is a copy at a particular point in time of data files to be backed up from the primary storage device and that was changed or added to the primary storage device after a previous backup. The incremental backup may be performed relative to a full backup or another incremental backup as is well understood by persons skilled in the art. Moreover, the previous backup from which an incremental backup is based need not be the most recent backup. This is further explained in the subsequent section.

g) *Enable Archive Log Mode:* This is a significant feature, where most DBA ignore it without or with intention. It is used to protect database logfiles from overwritten, as well as create archive log files based on the sequence number. Then, when crashed, failure or attack happened, the DBA can restore and recover the database system easily and safely.

h) *Forensic Soundness Assurance:* In compliance with the ISO/IEC 27043 standardization on incident response and investigation, a readiness approach is considered reliable when the burden of proof of admissibility can be substantiated. Several cryptographic mechanisms, particularly hashing algorithms, can be applied to the audit log to assure information integrity. By assuring the forensic soundness of the audit log and other logs within the readiness process, any potential evidence can be used to substantiate investigative claims.

i) *Prepare Recovery Plan and Alternative Workstation:* A company must have a robust recovery plan to recover database operations in the event of a disaster or crash happened. The absence of a recovery plan will cost the company a lot of money. Thus, the company must prepare alternative workstation to ensure the continuity of business, even the disaster or crash happened.

The procedure presented in Fig 3. provides a guideline for readiness, in anticipation of a potential incident, hence referred to as the pre-incident response. However, when a database incident has occurred, the next stage will be triggered which is termed *During-incident response*.

Stage II: During-Incident Response

The during-incident response stage is used to respond to the database incidents which have already taken place. A set of actions must be followed by the incident responder, to check and discover the database incidents:

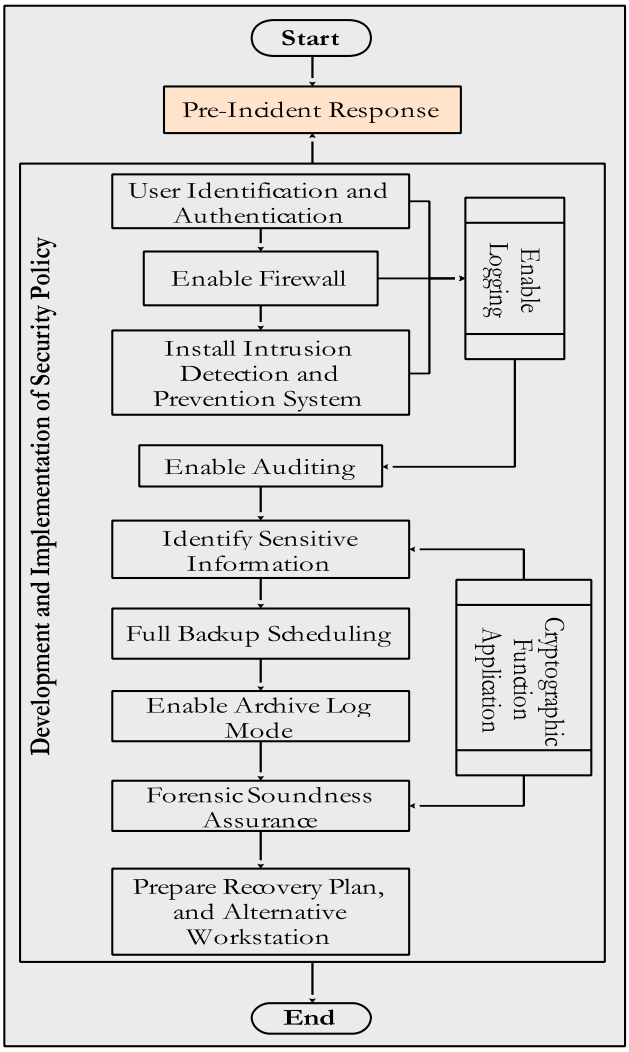

FIGURE 3. Pre-Incident Response.

1) *Isolate Database Server:* A database server should be disconnected from the users, while its entire processes and operation are suspended during the incident response phase. Database processes and operations are required to be suspended to capture evidence of an action that can be attributed to an intruder. This could involve stopping new access, stopping any or all current sessions as well as removing the database from existing usage (e.g., by disconnecting the database server from any network and/or direct connections). After isolating the database server and suspending whole user activities, incident responders must seize whole volatile and non-volatile data. The next procedure concentrates on live responses. The Isolating/disconnecting the suspect database server does not mean a shutdown of the database, however, isolating the users from the database management system.

2) *Perform Live Response*: When a database is cleanly shut down either by an attacker or an erroneous occurrence, the resultant effect, among other things, will

erase the content of the audit trail which induces further complexity to the investigation process. Particularly, the job of the forensic examiner is made more difficult by such an act or trigger. For reasons such as loss of volatile information, among other reasons, some organizations seek to prefer to perform an analysis on the system whilst it is powered on and connected to the network. This is typically referred to as Live Response. Live Response (LR) involves the process of recovering and safely storing volatile data for future analysis. Furthermore, LR provides a platform for the forensic examiner to acquire non-volatile evidence in a ''human-readable'' format which is easier to peruse than a stored binary equivalent–event logs for instance. All output from the Live Response tools can be written to a collection server across the network. Thus, the incident responder can follow these steps to achieve live response:

a) Record the system time and date of the system.
b) Identify the list of users that are currently logged on to the system: obtain a list of all users, gathering details on when they last logged in, and groups on the server and group membership.
c) Obtain a list of all running processes.
d) Obtain a list of the DLLs or shared objects that are loaded by each process. Keep an eye out for odd-looking names; on Windows lookout for DLLs that are loaded via a UNC path across the network.
e) Gather memory dumps of all running process even in what appear to be ''normal'' looking processes. The reason for this is to catch cloaking attacks. An attacker may launch a benign process like ''notepad'' and using CreateRemoteThread() load code into its address space.
f) Perform Dump all system memory. This will cover those bits of memory not dumped when dumping each process.
g) Get file names and MACTimes: The incident responder should perform a full recursive directory list of every disk and get file and directory names as well as their creation, access, and modification times. They should also gather information about each file's owner and any special attributes such as whether the read-only, system, or hidden attributes are set.
h) Perform dump of all Windows registry information.
i) Locate and take copies of log files and message logs: All Server log files and event and message logs should be copied to the collection server for analysis. These logs will vary from the system.
j) Acquire whole database files which are datafiles, control files, log files, redo log files, text files, binary files, archive files, and parameter files.
k) Acquire whole backup files which are logical backup sets, and physical backup sets.
l) Conduct Interview: the interview is used to collect data from the company staff members. Also, it is very useful to verify the existence of a server managed by the company as well as grasp server locations and accounting information besides basic information such as IP of the database server and service port numbers. The gathered data includes many data relating to database activity, physical log files, and file database server. Furthermore, these data include pieces of evidence of what the intruder did and metadata regarding the intruder's activity.

1. *Preserve Gathered Data:* The preserve gathered data is used to protect the integrity of data collected using hashing and backup methods, and also to prevent any modification of gathered data 15], [21]. Hashing is used to ensure that the gathered data does not change during forensic processes mainly through verification. Also, it assures the reliability of transferred gathered data between the source and the destination. Moreover, the backup concept provides an exact copy of data gathered that may use as a second copy when original data has been altered. Therefore, a copy of the hashed digest that is gathered data should be transferred to the forensic investigation environment through a secure channel to conduct reconstruction and analysis activities.
2. *Prepare Forensic Investigation Environment and perform an investigation task:* The preserved data gathered in Step 5, will be transferred to this station to perform investigation and search for evidence. This procedure includes two processes: prepare the forensic investigation environment & archive the investigation to search for evidence. The forensic investigation environment is a collection of the investigation team, processes, activities, tools, and methods used during the investigation task. Thus, this procedure includes these steps as illustrated in Fig 4.
    a) Organize a new machine: this includes a new secure workstation, server, or lab to conduct a final investigation.
    b) Install a new version of DBMS: the new DBMS must be similar to the destroyed database system in terms of version, files, and applications.
    c) Organize proper forensic methods/tools: the trusted and clean forensic methods/tools should be organized such as verification tools and methods, acquisition tools and methods, preservation tools and methods, reconstruction tools and methods, analysis tools, and methods.
    d) Import preserved gathered data: a copy of whole preserved gathered volatile and nonvolatile data must be imported to the new version of the DBMS.

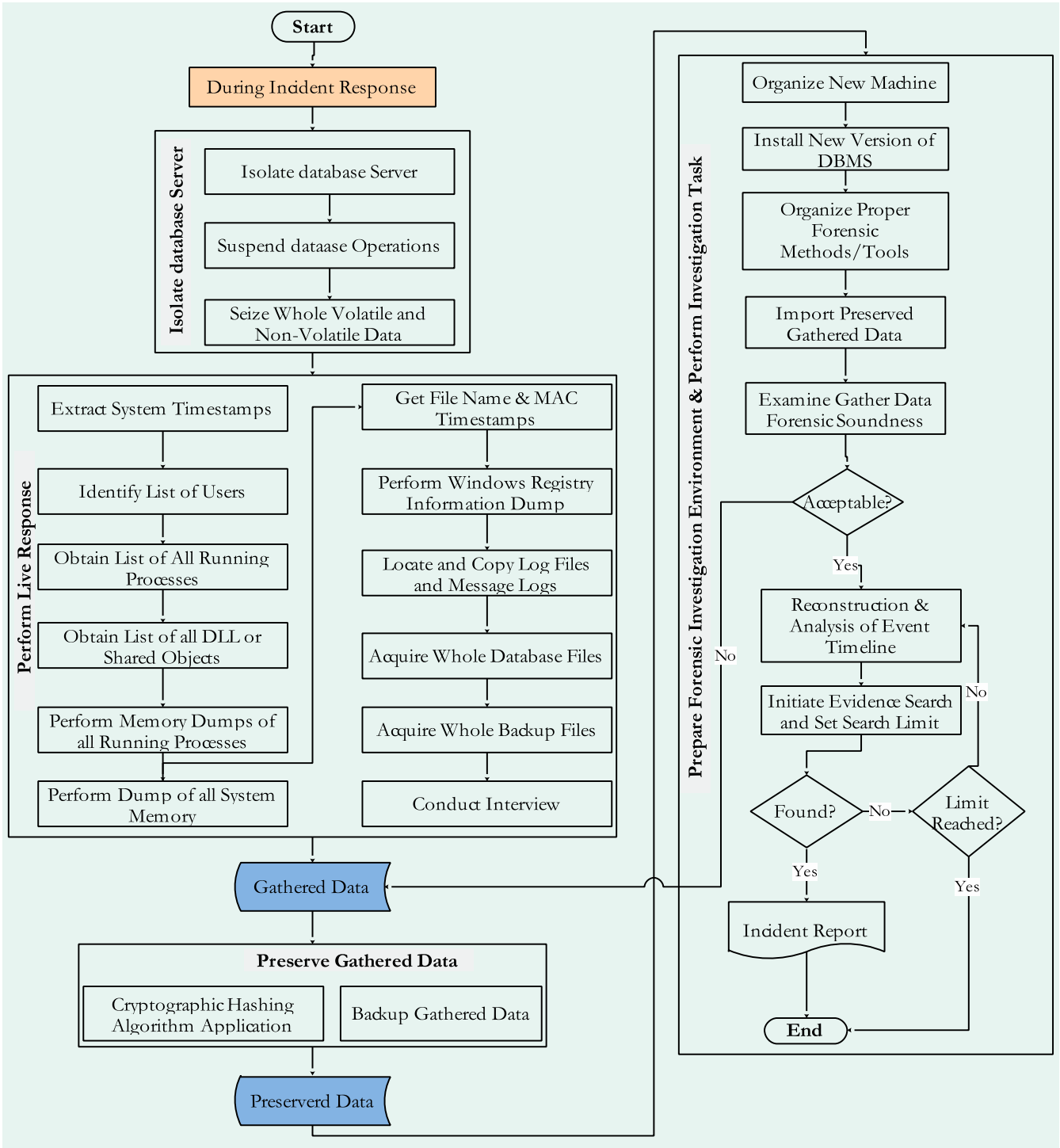

FIGURE 4. During Incident Response Stage.

e) Examine gathered data: it is used to ensure that data gathered is authentic and has not been tampered with. Thus, the first mission of the investigation team is to examine the authenticity of data gathered using such forensic techniques. However, if the gathered data has been modified, the investigation team must bring another clean data gathered from the originally gathered data.

f) *Reconstruction and analysis timeline events*: The reconstruct is used to rebuild timeline events from gathered volatile and non-volatile data which involves retracing past system, user database

activity, past SQL execution history, stored procedures, and function execution. The investigation team performs a reconstruction process using forensic techniques such as Log Miner, forensic algorithms, or Dragon. Timeline events are a collection of digital events that have been recognized from the reconstruction process that will be used during analysis. For an example of digital events that have been recognized: failed login events, successful login events, malicious database events that can be recognized and added to an examination timeline. Furthermore, creating a timeline of events can assist an investigator to gain insight into the events that occurred, and the people involved. Finally, the investigation team documents the whole reconstruction procedure in several reports and should be submitted to the company or the court. Whole procedures of the pre-incident response and during should be evaluated and enhancement periodically, to improve and develop the incident responding model.

g) *Search for Evidence*: The reconstructed timeline events searches and filters using such forensic tools/methods to offer the pieces of evidence. Pieces of evidence are usually recognized in the database files that are recorded on hard drives and storage devices and media [26]. It is transmitted in binary form that may be relied upon in court. It consists of who, why, when, what, how, and where the malicious transactions were carried out.
h) *Incident Report*: After the investigation of database incidents is finished, all the findings and results have to be documented in a written report. In such a report, the investigation processes have to be documented, and all conclusions drawn should be explained. Such a report should be presented in a concise, and intelligible manner which can be read by a non-technical user. Given the results of the report might be used as evidence during a lawsuit, the report should be able to hold up against legal scrutiny.
i) *Restore and Recover Database Operations:* After finishing the investigation and fix the problem, the database system should be open for normal operations. Thus, the clean backup which has been taken in the pre-incident response should restore and recover whole recent activities from the clean incriminate archive log files.
j) *Open Database Server:* when database recovered successfully, the database server should be open for database users.

Stage III: Post-Incident Response

This stage is the final stage after an incident has been checked and resolved, which illustrated in Fig 5. Post-incident is primarily focused on gathering information

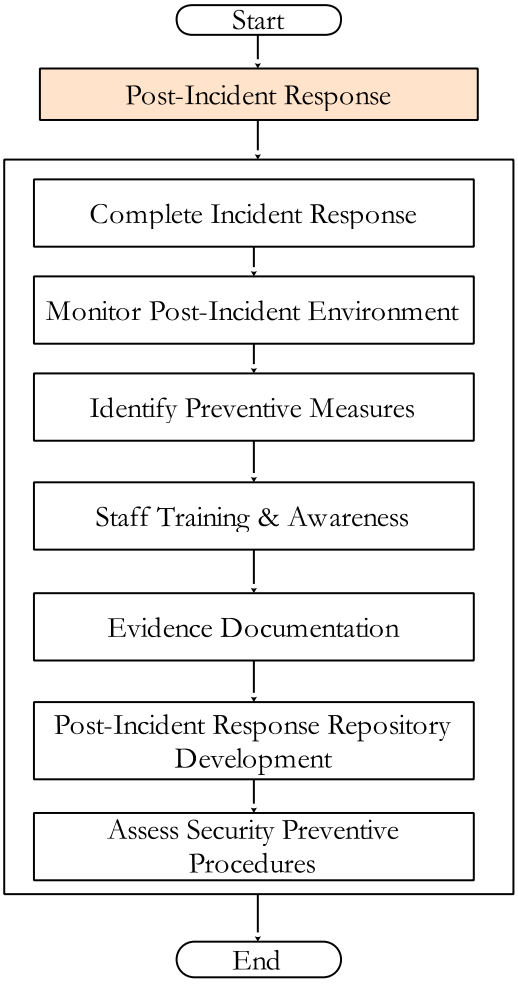

FIGURE 5. Post-Incident Response.

from the two previous stages (pre-incident response and during-incident response) for learning and enhancing objective, and generally take the form of a report. It also includes official reporting to top-management and advising enhancements in incident managing from practical and administrative views. The findings from the second stage will be contained as one of the necessary reports in this stage. The content will consist of the documentation gathered during the incident stage, the analysis methods and tools, and other important findings. The report can also be submitted to a court or for additional legal procedures. Therefore, this stage has these procedures:

a) *Complete an incident report:* Documenting the incident will help to improve the incident response plan and augment additional security measures to avoid such security incidents in the future: how logging is done; what is logged; what are the intrusion detection systems (IDS); what are the forensic preparation, acquisition, reconstruction and analyzing methods, tools;
b) *Monitor Post-Incident:* closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM

TABLE 3. Comparing of IIRM Stages.

Pre-incident Response	During-Incident Response	Post-Incident Response
1. Protect the confidentiality, integrity and availability of the database systems using robust security policies. 2. Apply security alerts and enable auditing to avoid destroy database contents. 3. Prepare backup strategies to use it as an investigation resource when database incidents would happen. 4. Prepare comprehensive investigation environment 5. Prepare full recovery plan	1. Isolate whole or part of destroyed database server to stop database activities. 2. Collect volatile and nonvolatile data. 3. Preserve collected volatile and nonvolatile data. 4. Examine the authentication of the collected data. 5. Reconstruct, and analyze collected data and highlighted evidences. 6. Prepare incident report.	1. Documenting the incident to help incident responders to enhance the incident response plan and augment additional security measures to avoid such security incidents in the future. 2. Monitor for actions post-incident 3. Establish new security plans to prevent future incidents. 4. Train staff to understand their role in the digital evidence process and the legal sensitivities of evidence. 5. Develop a post-incident response repository to store the entire knowledge of the database incidents.

data for any signs of indicators tripping that may have been associated with the prior incident.

c) *Identify preventative measures:* Create new security initiatives to prevent future incidents.

d) *Train staff:* The staff must be trained in incident awareness so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.

e) *Evidence Documentation*: Document an evidence-based case by describing the incident and its impact. Ensure legal review to facilitate action in response to the incident.

f) *Develop a post-incident response repository*: A repository is used to store the entire knowledge of the database incidents. The repository investigation team to mix and match previous knowledge and use it in several similar cases.

g) *Assess security preventive procedures*: Create new security preventive procedures to prevent future incidents.

A summary analysis of the respective stages of the incident response process is further presented in Table 3. The comparison reflect the composition of each stage relative other stages.

V. RESULTS AND DISCUSSION

Comparing to the existing database incident models, which focused purely on technical investigation purposes such as detection incident, collection data, preserving, reconstruction, analysis, and documentation, this study proposed a new incident response model which is further termed as IIRM. It is a hybrid model that consists of four main goals: establish a plan to avoid any database disaster, investigate and search for potential evidence, recover database operations, and finally sharing database disaster knowledge. These four stages are further explained:

1. *Establish a plan to avoid any database disaster:* most database incidents/disasters as revealed in existing literature show that a database system has no robust incidents response strategies to avoid insider or outsider attacks. Breaches and attacks on database infrastructures have been reported in few organizations, at different times. This has been partially attributed to the misuse of existing database frameworks and vulnerabilities such as SQL infusion blemishes and unpatched databases. Whilst most attacks have been attributed to outside hackers, other subtle and more catastrophic attacks have been attributed to insiders and the lack of appropriate standardization. Such include data breaches, the lack of data regulations, bad accounting practices, fraud, and various corporate scandals and crimes. However, these vulnerabilities and susceptibilities can be mitigated through the enforcement of standardized regulations and processes proposed in the pre-incident response stage, as discussed in Section-III, of this manuscript.
2. *Investigate and search for evidence:* the second goal of the IIRM is to search for potential evidence that can be used to uncover database incidents. This phase represents the integration of various activities of the incident-handling phases of most database investigation models. Thus, activities such as disconnecting database servers, suspended database operations, gathering, and preserving data, event reconstruction, data analysis, as well as investigation documentation have been combined in this stage.
3. *Recovering database operations:* The third goal of the IIRM is to restore and recover database systems and open it for normal operations. The equipment and evidence collected are returned to their respective owners.
4. *Sharing database disaster knowledge:* The fourth goal of the proposed IIRM is to share the database incident information among domain practitioners. This phase of knowledge dissemination and or acquisition is crucial to the continuity and effectiveness of the investigation. Here, feedback and appropriate action are communicated to relevant authorities to foster collaboration, clarification of ambiguities of the result, and documentation. Furthermore, information from this phase can be used to provide a reference for future incidents, coming from the knowledge extracted from the current incident and investigation process.

As highlighted in Section I of this manuscript, the fundamental questions on who should respond to an incident in a database incident is an important aspect of the incident response process. Answer to this question is articulated in Stage I of the proposed IIRM. Furthermore, the sequence

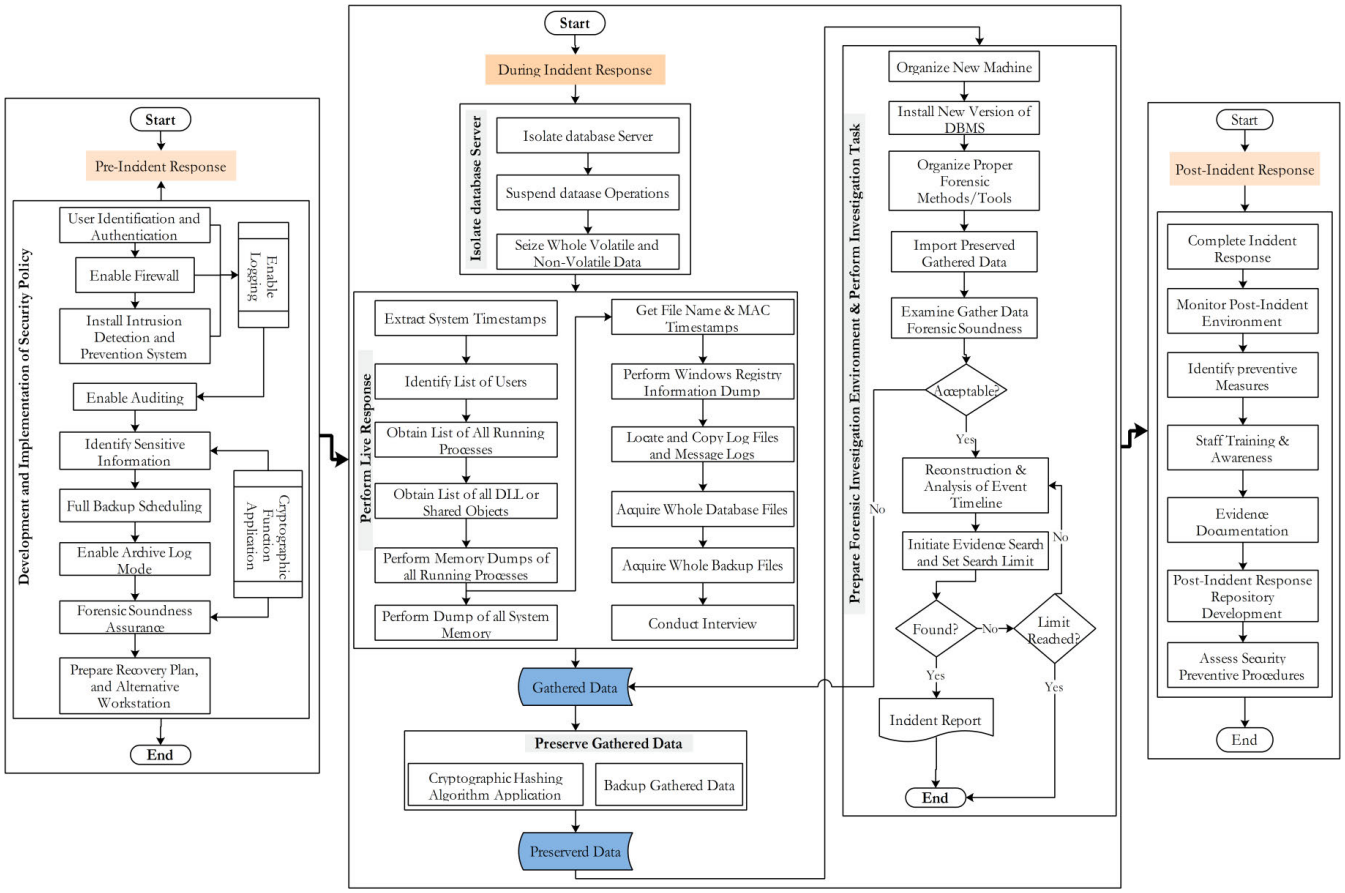

FIGURE 6. Integrated framework of the proposed IIRM.

of the processes to follow, particularly for first responders, in a database related crime/incident is clearly defined in Stage II of the proposed models. These phases of the model can be extended to align with the digital forensic readiness phase of the ISO/IEC 27043 standards [26]. Forensic readiness as defined in existing literature could introduce a standardized approach to potential evidence reliability and extraction before incident occurrence (pre-mortem). Therefore, the phases of the pre-incident response of the proposed model can be further extended to accommodate organization preparedness against database downtime whilst providing reliable content that could otherwise have been lost. An example of this assertion is the collection of volatile information and the running configuration of a database. This assertion, therefore, answers the fourth question stated in Section I of this manuscript. The answer posits that the integration of a methodical approach towards potential evidence identification, collection, and storage in a pre-incident can be used to reliable address the problem of volatile evidence preservation. Another core fundamental composition of the proposed IIRM is the integration of forensic soundness into database incident investigation. As highlighted by studies in [7], [9], the forensic soundness assurance can provide a reliable corroborative substance, beyond any reasonable doubt, given that the chain-of-custody, and chain-of-analysis can be proven at any requested time. Furthermore, the integrity and reliability of any potential evidence are ensured within the pre-incident and during incident response processes. The integrated framework of the proposed IIRM is further presented in Fig 6. The output from Stage I is primarily defined as the input to Stage II where chain-of-custody and chain-of-evidence are ensured respectively. The last Stage III addresses management concerns, proactive measure development, as well as post-incident planning processes. Often, the post-incident process is relegated to an afterthought which, potentially, leads a repeated database incident. Therefore, the proposed model can be defined as a comprehensive model that could be used to pre-empt, prepare for, and prevent a database incident occurrence.

Without discounting the aforementioned capabilities of IIRM, the authors of this paper takes a stept to explore the advantages of IIRM that supersedes the existing models as well as the limitations. It is important to beforehand note that, the limitation that have been identified have carefully been analysed and positioned to be relevant for inclusion as future work.

The IIRM has been juxtaposed as a comprehensive model-which has major inclusion and integration of processes

that have been suggested by existing database investigation models. While it is important to acknowledge that these models have offered very significant insights towards the development of IIRM, we put across one core advantage that IIRM holds. IIRM is able to cover pre-incident preparation that has explicitly been presented at a readiness phase [3], this phase not only is able to shorten the process of conducting investigation in databases but also it saves time due to the availability of forensic evidence when needed. As far as IIRM is concerened this would be executed by implementing security policies as was mentioned and highlighted previously in Figure 3. Additionally, the scope of the major phases in the proposed IIRM (Pre-incident Response, During Incident Response and Post-incident Response) have been described well based on their functionalities, where IIRM hold an advantage of leveraging the prescribed guidelines for information technologies, incident investigation techniques and processes that explicitly are adapted verbatim from ISO7IEC 27043 [3]. Next, the IIRM has room for further integration, which means it is easy to incorporate other suitable processes because of how the different phases have been classified and as a result the IIRM endeavors to accept other processes that can be deemed as essential during integration.

At the time of writing this paper, there currently does not exist, specific guidelines or standards that address incident response categorically and as such, incident response can only be encapsulated in ISO/IEC 27043 investigative process classes from a generic perspective. This, is a current limitation of this model, however, an inclusion or adoption of these (standardised)guidelines will be inevitable.

VI. CONCLUSION

As part of an ongoing process, this study presented a core component of the integrated database investigation model; the incident response phase. The design science approach was considered essentially appropriate to carry out this study, and the resulting procedure, capable of establishing an incident-response baseline for database forensics, has been developed. The developed incident response model comprised three interdependent phases which include the pre-incident response, During-incident response, and post-incident response phases respectively. The notion of evidence reliability and forensic soundness was identified and ensured for each phase. Consideration of the other components of the integration database forensic model, as well as the interactivity among each component, will be further examined in future studies. These will comprise the process of ascertaining and maintaining evidence reliability across the broad phases of a typical metamodel, and the management of database forensic entities.

REFERENCES

[1] G. Grispos, W. B. Glisson, and T. Storer, "How good is your data? Investigating the quality of data generated during security incident response investigations," 2019, *arXiv:1901.03723*. [Online]. Available: http://arxiv.org/abs/1901.03723

[2] M. Malik and T. Patel, "Database security–attacks and control methods," *Int. J. Inf. Sci. Techn.*, vol. 6, nos. 1–2, pp. 175–183, Mar. 2016.

[3] *Information Technology—Security Techniques—Incident Investigation Principles and Processes*, document ISO/IEC 27043, 2015.

[4] V. R. Kebande and H. S. Venter, "On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges," *Austral. J. Forensic Sci.*, vol. 50, no. 2, pp. 209–238, Mar. 2018.

[5] A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital forensic readiness framework for ransomware investigation," in *Digital Forensics and Cyber Crime*. Midrand, South Africa: Springer, 2019, pp. 91–105.

[6] A. Singh, H. S. Venter, and A. R. Ikuesan, "Windows registry harnesser for incident response and digital forensic analysis," *Austral. J. Forensic Sci.*, vol. 52, no. 3, pp. 337–353, 2020.

[7] H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness approach for potential evidence preservation in software-defined networks," in *Proc. 14th Int. Conf. Cyber Warfare Secur. (ICCWS)*, 2019, pp. 268–276.

[8] D. Ellison, H. Venter, and A. Ikuesan, "An improved ontology for knowledge management in security and digital forensics," in *Proc. Eur. Conf. Cyber Warfare Secur.*, 2017, pp. 725–733.

[9] A. R. Ikuesan and H. S. Venter, "Digital forensic readiness framework based on behavioral-biometrics for user attribution," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2017, pp. 54–59.

[10] J. C. Odirichukwu and P. O. Asagba, "Security concept in Web database development and administration—A review perspective," in *Proc. IEEE 3rd Int. Conf. Electro-Technol. Nat. Develop. (NIGERCON)*, Nov. 2017, pp. 383–391.

[11] M. S. Olivier, "On metadata context in database forensics," *Digit. Invest.*, vol. 5, nos. 3–4, pp. 115–123, Mar. 2009.

[12] D. Wong and K. Edwards, "System and method for investigating a data operation performed on a database," U. S. Patent 2005 0 289 187 A1, Dec. 29, 2005.

[13] K. Fowler, G. M. Gold, and M. Mcsd, "A real world scenario of a SQL server 2005 database forensics investigation, information security reading room paper," SANS Inst., Bethesda, MD, USA, 2007.

[14] D. Litchfield, "Oracle forensics part 4: Live response. NGSSoftware insight security research (NISR)," Next Gener. Secur. Softw. Ltd., Sutton, U.K., Tech. Rep., 2007.

[15] K. Fowler, *SQL Server Forenisc Analysis*. London, U.K.: Pearson, 2008.

[16] D. Lee, J. Choi, and S. Lee, "Database forensic investigation based on table relationship analysis techniques," in *Proc. 2nd Int. Conf. Comput. Sci. Appl.*, Dec. 2009, Art. no. 5404235.

[17] J. Choi, K. Choi, and S. Lee, "Evidence investigation methodologies for detecting financial fraud based on forensic accounting," in *Proc. 2nd Int. Conf. Comput. Sci. Appl. (CSA)*, Dec. 2009, Art. no. 5404202.

[18] N. Son, K.-G. Lee, S. Jeon, H. Chung, S. Lee, and C. Lee, "The method of database server detection and investigation in the enterprise environment," in *Proc. FTRA Int. Conf. Secure Trust Comput., Data Manage., Appl.* Berlin, Germany: Springer, 2011.

[19] S. Tripathi and B. B. Meshram, "Digital evidence for database tamper detection," *J. Inf. Secur.*, vol. 3, no. 2, p. 113, 2012.

[20] H. K. Khanuja and D. Adane, "A framework for database forensic analysis," *Comput. Sci. Eng.*, vol. 2, no. 3, p. 27, 2012.

[21] R. Susaimanickam, "A workflow to support forensic database analysis," Murdoch Univ., Murdoch, WA, Australia, Tech. Rep., 2012.

[22] O. M. Fasan and M. S. Olivier, "On dimensions of reconstruction in database forensics," in *Proc. WDFIA*, 2012, pp. 97–106.

[23] H. Q. Beyers, "Database forensics: Investigating compromised database management systems," Univ. Pretoria, Pretoria, South Africa, Tech. Rep., 2014.

[24] 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," Univ. Nairobi, Nairobi, Kenya, Tech. Rep., 2017.

[25] H. K. Khanuja and D. D. S. Adane, "Forensic analysis of databases by combining multiple evidences," *Int. J. Comput. Technol.*, vol. 7, no. 3, pp. 654–663, Jun. 2013.

[26] H. Khanuja and S. S. Suratkar, "Role of metadata in forensic analysis of database attacks," in *Proc. IEEE Int. Advance Comput. Conf. (IACC)*, Feb. 2014, pp. 457–462.

[27] 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," *Digit. Invest.*, vol. 11, no. 4, pp. 336–348, Dec. 2014.

[28] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quart.*, vol. 28, no. 1, pp. 75–105, 2004.
[29] S. H. Othman, G. Beydoun, and V. Sugumaran, "Development and validation of a disaster management metamodel (DMM)," *Inf. Process. Manage.*, vol. 50, no. 2, pp. 235–271, 2014.
[30] O. M. Adedayo and M. S. Olivier, "Ideal log setting for database forensics reconstruction," *Digit. Invest.*, vol. 12, pp. 27–40, Mar. 2015.
[31] J. Wagner, A. Rasin, and J. Grier, "Database forensic analysis through internal structure carving," *Digit. Invest.*, vol. 14, pp. S106–S115, Aug. 2015.
[32] A. Al-Dhaqm, S. A. Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," *J. Teknologi*, vol. 78, nos. 6–11, Jun. 2016.
[33] A. Al-Dhaqm, S. Razak, S. H. Othman, K.-K.-R. Choo, W. B. Glisson, A. Ali, and M. Abrar, "CDBFIP: Common database forensic investigation processes for Internet of Things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017.
[34] R. Bria, A. Retnowardhani, and D. N. Utama, "Five stages of database forensic analysis: A systematic literature review," in *Proc. Int. Conf. Inf. Manage. Technol. (ICIMTech)*, Sep. 2018, pp. 246–250.
[35] 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 Cognit. Archit.*, vol. 9, pp. 82–104, Jul. 2014.
[36] A. C. Bogen and D. A. Dampier, "Preparing for large-scale investigations with case domain modeling," in *Proc. DFRWS*, 2005, pp. 1–10.

ARAFAT AL-DHAQM (Member, IEEE) received the B.Sc. degree in information system from the University of Technology-Iraq, the M.Sc. degree (Hons.) in information security and the Ph.D. degree in computer science from the Universiti Teknologi Malaysia (UTM). He holds a Postdoctoral Fellowship position with UTM. His Ph.D. research focused on solving the heterogeneity and ambiguity of the database forensic investigation field using a meta-modeling approach. His current research interests include span the domains of digital forensics and cybersecurity.

SHUKOR ABD RAZAK (Member, IEEE) is currently an Associate Professor with the Universiti Teknologi Malaysia. He is the author or coauthor of many journals and conference proceedings at national and international levels. He is actively conducts several types of research in digital forensic investigation, wireless sensor networks, and cloud computing. His research interests include security issues for mobile ad hoc networks, mobile IPv6, vehicular ad hoc networks, and network security.

KAMRAN SIDDIQUE (Member, IEEE) received the Ph.D. degree in computer engineering from Dongguk University, South Korea. He is currently an Assistant Professor with Xiamen University Malaysia. His research interests include cybersecurity, machine learning, and big data processing.

RICHARD ADEYEMI IKUESAN received the M.Sc. and Ph.D. degrees (Hons.) in computer science from the Universiti Teknologi Malaysia. He is currently an Assistant Professor with the Cyber Security Section, IT Department, Community College of Qatar. He is also an Active Researcher pioneering a digital policing and forensic project for developing nations, using Nigeria and South Africa as a hub for West Africa and Southern Africa, respectively.

VICTOR R. KEBANDE received the Ph.D. degree in computer science (information and computer security architectures and digital forensics) from the University of Pretoria, Hatfield, South Africa. He was with ICSA and DIgiFORS Research Groups, University of Pretoria. He is currently a Postdoctoral Researcher in cyber and information security with the Internet of Things and People (IoTaP) Center, Department of Computer Science and Media Technology, Malmö University, Sweden. His main research interests include cyber, information security and digital forensics in the area of the IoT, (the IoT security), digital forensics-incident response, cyber-physical system protection, critical infrastructure protection, cloud computing security, computer systems, distributed system security, threat hunting and modeling and cyber-security risk assessment, blockchain technologies, and privacy preserving techniques. He also serves as an Editorial Board Member for *Forensic Science International* (Reports Journal).