CIPM: Common Identification Process Model for Database Forensics Field

Ibrahim M Alfadli
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
ialfadli@taibahu.edu.sa

Fahad M Ghabban
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
fghaban@taibahu.edu.sa

Omair Ameerbakhsh
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
oameerbakhsh@taibahu.edu.sa

Amer Nizar AbuAli
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
aabuali@taibahu.edu.sa

Arafat Al-Dhaqm
Faculty of Engineering, School of Computing,
University Technology Malaysia
Malaysia, Johor
mrarafat1@utm.my

Mahmoud Ahmad Al-Khasawneh
Faculty of Computer & Information Technology
Al-Madinah International University
Shah Alam, Malaysia
mahmoud@outlook.my

Abstract— **Database Forensics (DBF) domain is a branch of digital forensics, concerned with the identification, collection, reconstruction, analysis, and documentation of database crimes. Different researchers have introduced several identification models to handle database crimes. Majority of proposed models are not specific and are redundant, which makes these models a problem because of the multidimensional nature and high diversity of database systems. Accordingly, using the metamodeling approach, the current study is aimed at proposing a unified identification model applicable to the database forensic field. The model integrates and harmonizes all exiting identification processes into a single abstract model, called Common Identification Process Model (CIPM). The model comprises six phases: 1) notifying an incident, 2) responding to the incident, 3) identification of the incident source, 4) verification of the incident, 5) isolation of the database server and 6) provision of an investigation environment. CIMP was found capable of helping the practitioners and newcomers to the forensics domain to control database crimes.**

Keywords— Database forensics; Identification process; digital forensics, metamodelling

I. INTRODUCTION

Database Forensics (DBF) is a field classified under the digital forensics field of study, which inspects database content with the aim of verifying database crimes [1]. DBF is well recognized as a field of high significance because it can identify, detecting, acquiring, analyzing, and reconstructing incidents that occur in a database, thereby determining the intruders' activities. On the other hand, it suffers from several problems due to which DBF is known as an unstructured field of heterogeneity and confusion [2], [3]. For instance, it involves various database system infrastructures, the database systems are generally multidimensional, and the knowledge domain is scattered in all directions [4]. Different infrastructures of the database system with a multidimensional nature help DBF to deal with specific incidents. As a result, each database management system (DBMS) has different identification investigation model/approach. For that reason, the issues of forensic investigation processes and the scattering of knowledge in all directions have led to some other problematic areas for practitioners and researchers working in the DBF field [2], [5], [6]. This knowledge includes models, techniques, processes, tools, activities, methods, frameworks, algorithms, and approaches) is generally disorganized and non-structured. In addition, this is dispersed at a universal level, for instance, on the Internet, journals, books, reports, online databases, conferences, dissertations, and organizations. As a result, the literature lacks identification models capable of unifying the concepts and terminologies in a way to lessen the existing confusion and help in making domain knowledge well organized and structured [7]–[13]. As various infrastructures exist for DBMS, several DBF process models have been introduced in the literature to manage the field of DBF from the perspective of the investigation process [14]–[17] Nonetheless, among them, no single model can be found to be applied as a common model to the DBF field. The process models are typically applied to solving certain database incidents, case studies, or scenarios. For that reason, these models have generated processes of high redundancy and irrelevancy.

The models introduced in this field have addressed DBF from four perspectives of investigation processes: 1) identification process, 2) collection process, 3) analysis process and 4) presentation process. In the current study, the identification process perspective is discussed in detail. The models discussing DBF from an identification process perspective typically hold different and redundant investigation processes, tasks, and activities. The *Suspension of Database Operation* process provided in the model proposed in [18], [19] works by isolating the database server from the users to capture database activities. However, the *Verification* and *System Description* processes provided in the model introduced in [20] works by verifying the database incidents, isolating the database server, confirming the incident, documenting the system information like the name of the system, operating system, serial number, system function, and physical descriptions. Moreover, the *Identification* process suggested in the models proposed in [21], [22] indeed disconnects the database server from the network to capture volatile data. Similarly, the *Incident verification* and *Investigation preparation* processes proposed in [23] are aimed at identifying and verifying the database incidents by a preliminary investigation. These models then provide forensic workstations and toolkits to give a response to the incidents; then, they disconnect the database server. Additionally, the *Database Connection Environment* introduced by the authors in [24] prepares the investigation environment, gains permission for having access to the database, and executes the commands needed. Moreover, the *Table Relationship Search and Join process* is mainly aimed at extracting the tablespaces within the database, choosing the target, selecting the tables storing the investigation data, and checking recurrently the other table field. In the *Data Acquirement with Seizure and Search Warrant* process, there is a need to secure the evidence location and extract the evidence related to a certain crime or incident [24], [25]. *Server Detection* is another process of interest, which detects the server that runs a database system. This process grasps the overall network environment in a firm. It acquires the network topology in the firm, which is applied to the identification and detection of the victim database server [26]–[28]. The researchers in [29] described the *Setup Evidence Collection Server* process that was employed to prepare the investigation environment for storing the incidents, whereas the *Identification* process introduced in [30] is used to identify the relevant MySQL database files (log files, text files, binary files) and utilities. Likewise, in [31], [32], the *Incident reporting and Examination Preparation* processes were introduced to capture database incidents utilizing the users' reports, system audit, or triggered events. To discover the database incidents, they cut off the network, configure the investigation circumstance, identify policies, prepare the appropriate tools, and inform the decisions made. Furthermore, the authors in [33] proposed the *Determining Database Dimension* and *Acquisition Method process* to identify the dimensions of a database that has been hacked/attacked. After that, the appropriate acquisition methods for that dimension are determined. In addition, the *Choose environment and Select implement method* process

suggested in [34] choose the forensic context (clean or found environment) and choose an approach to transforming the forensic setting into the chosen forensic setting. The *Preliminary analysis* process introduced in [27], [35], [36] was implemented with the aim of forming an architectural visualization of DBMS with all components and their locations in the layered model of DBMS, identifying the files and folders in the layers below the storage engines' layer, preparing and utilizing the forensic tools and processes for the creation of an initial image and then the collection of metadata values of the identified target files, and recording the metadata of the target files [8], [37], [38]. Accordingly, the current study is mainly aimed at integrating all exiting identification process tasks and activities into an identification process model applicable to DBF with the use of the metamodeling approach, called CIPM. It comprises three phases: 1) Pre-identification, 2) During-identification, and 3) Post-identification. The three phases, in turn, comprise a number of steps and processes aiming to provide the techniques, tools, strategies, policies, and methods of investigation [38], which are implemented for the purpose of identifying, gathering, preserving, analyzing, and documenting database crime. CIPM has the capacity of structuring, unifying, facilitating, managing, sharing, and reusing the DFI field knowledge amongst the practitioners working in the forensics field. The metamodeling approach identifies the general concepts existing within each problem domain and examines the relationships among them. It makes a less complex, less interoperable, and less heterogeneous domain [39], [40]. As a result, the metamodels/models need to be defined meticulously and structured properly.

Therefore, the rest of this paper is arranged as follows: Section 2 discusses the methodology and Section 3 presents the initial results and discussion, and finally, Section 4 concludes the whole study.

II. METHODOLOGY

In designing CIPM, five steps of the metamodeling creation process were adapted as presented in [41] (see Fig. 1).
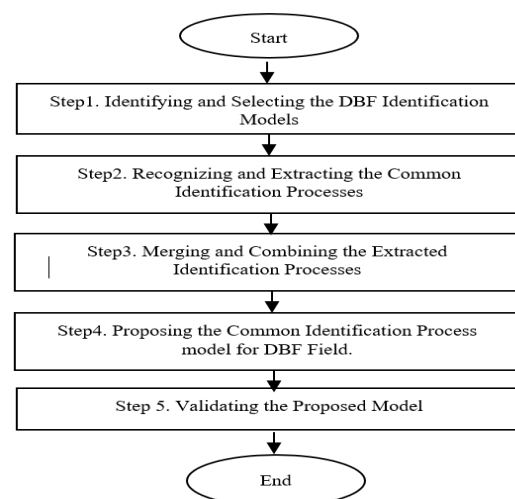

Fig. 1. Metamodeling development process

73

Step 1. Identifying and Selecting the DBF Identification Models: This step identifies and selects the production and validation models. Several DBF identification models proposed in the current literature were analyzed [42]–[44] In this paper, the model selection process was done based on the coverage factors identified in former studies. This step results in 19 identification models that can be applied to developing and constructing purposes (see Table I).

TABLE I. Development Models and extracted processes

Models	Database Forensic Identification Models	Similar Process
M1	[18]	Suspend Database Operations
M2	[20]	Verification
M3	[21]	System Description
M4	[23]	Identification process
M5	[24]	Identification process
M6	[45]	Investigation Preparation
M7	[46]	Incident Verification
M8	[26]	Database Connection Environment
M9	[29]	Table Relationship Search and Join Process
M10	[30]	Data Acquirement with Seizure and Search Warrant
M11	[31]	Server Detection
M12	[33]	Setup Evidence Collection Server
M13	[47]	Incident reporting
M14	[48]	Examination Preparation
M15	[49]	Determine Database Dimension
M16	[50]	Determining Acquisition Method
M17	[51]	Identification
M18	[52]	Preliminary analysis

Step 2. Recognizing and Extracting the Common Identification Processes: A DBF identification process resulted from the 18 models chosen earlier. Throughout this process, definite criteria were used for the identification of the relevant and appropriate identification processes. The criteria applied to determine the identification processes were taken from [53]–[55]. The criteria were used to avoid any missing or random process selections. Thus, in this section, a total of 18 identification processes were determined and derived from those 18 DBF identification models (see Table I).

Step 3. Merging and Combining of the Extracted Identification Processes: This step involves merging and combining the 18 extracted processes based on similarity in semantic meaning or functional meaning [56], [57]. All identification processes that have identical semantic meaning or functional meaning are organized into an abstract model called Common Identification Process Model (CIPM).

Step 4. Proposing CIPM for the DBF Field: This step introduces CIPM to be applied to the DBF field with the help of the mapping process. CIPM comprises three stages as demonstrated in Fig. 2.

Step 5. Validating the Proposed Model: CIPM is validated and enhanced to make it perfect and coherent as much as possible. To this end, the model is compared to identical existing models [56], [58].
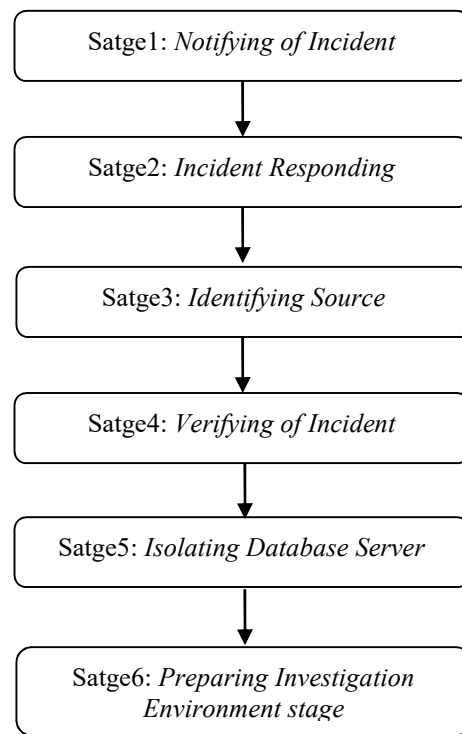

Fig 2. Common identification process model (CIPM)

III. RESULTS AND DISCUSSION

All DBF identification models, processes, tasks, and activities that appeared on the Internet, conferences, journals, online databases, books, and dissertations are specific and redundant. As a result, in the current paper, a common identification process model (CIPM) was designed in a way to be well applicable to the DBF field (see Fig. 1). It was attempted to include all the advantages of the previously proposed models in CIPM. It was properly defined in terms of meaning, tasks, and activities. This model is mainly aimed at solving the DBF field identification processes of irrelevancy and redundancy that tend to confuse practitioners working in the forensics domain. CIPM covers all the strengths of the models formerly proposed in the literature (see Table II). For example, the proposed Identification *process* contained whole investigation tasks, activities, and methods, of the eighteen (18) existing identification processes. Note that, in the present paper, *process* refers to respective stages that a scientific framework/model applies to the achievement of the most important goals, which is, in the case of the current study, producing an admissible forensic hypothesis applicable during the litigation process [43], [59].

TABLE II.   A COMPARATIVE SUMMARY: PROPOSED COMMON IDENTIFICATION PROCESS AGAINST VALIDATION MODELS

Proposed Common DBF Process	Existing DBF Models																	
	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12	M 13	M 14	M 15	M 16	M 17	M 18
Identification process	√	√	√	×	√	√	×	√	√	√	√	×	√	√	×	×	×	×

As can be seen in Fig. 1, this comprises six stages: notifying of the incident, responding to an incident, identification of the source, verification of incident, isolation of the database server, and preparation of investigation environment. In the first stage, the DBA of the firm notifies the higher management staff (for instance, Chief Executive Officer (CEO), Chief Security Officer (CSO), Chief Operating Officer (COO)) concerning the incident occurred to the database server [50]. When it occurs, the firm CEO has two choices [23]: assigning an internal/external investigation team for performing required investigations on the incident or stopping the investigation [23]. In case of the first option, the team will perform the second stage of the identification investigation process (i.e., the Incident Responding Stage) with the aim of collecting detailed data related to the incident, e.g., information in regard to the incidence of the event, parties involved, and the number of the databases involved associated with their sizes [20], [23]. To this end, the team applies forensic techniques for the purpose of seizing the investigation sources [24], collects the instable artefacts [21], and also collect helpful information by holding different interviews with the staff [26]. Incident Responding [22], [60], in turn, comprises three concepts: Capture, Live Response, and Interview. Accordingly, the investigation team captures the investigation sources, for instance volatile and non-volatile artefacts [21]. In addition, the Live Response is related to the concept of Volatile Artefact. As a result, the team collects useful volatile data from the Volatile Artefact concept. The last concept addressed in the Incident Responding is Interview. The team is required to carry out some interviews with the firm's senior staff (e.g., CEO and DBA) [26]. These interviews may result in collecting basic information, e.g., information accounts, database server, users, network ports, incident reports, investigation processes, logs, and policies [26]. It is clear that the incident responding stage helps the team determine an incident boundary and also decide about the investigation sources[61], [62]. The third stage involves Identifying Source Stage through which specific investigation sources are identified [21], [23], [30]. In an investigation source, there may be several helpful volatile and non-volatile artefacts that hold valuable evidence. As a result, this stage addresses the concepts captured during the responding stage (e.g., Artefact, Volatile Artefact, Nonvolatile Artefact, Source, Log File, Database File, and Undo Log concept). Then, the next investigative stage is dedicated to Verifying of Incident stage, which helps the team verify the incident occurred to the database [20], [23]. This stage comprises nine main concepts: Investigation Team, Incident, Destroyed Database, Modified Database, Compromised Database, Incident Types, Report, Company, and Decision. Thus, the team need to identify the type of the incident (is it compromised, destroyed, or modified)

[33], the nature of the incident, and the status of the incident. After that, the team will submit a detailed report the firm management in regard to the incident to [24]. Managers will review the report submitted and, accordingly, make necessary decisions; three options exist: keeping on the investigation process, stopping the process, or disconnecting the database server from the network [21], [31]. When the incident is completely verified and determined, then fifth stage, i.e., Isolating Database Server, starts. Through this stage, the team has the ability of isolating/disconnecting[61], [62] a suspect database server from the network with the aim of avoiding more tampering [18], [23]. This stage comprises three concepts: Investigation Team, Database Server, and Database Management System. Note that isolating or disconnecting the suspect database server does not necessarily result in the database shutdown [21]; rather, it isolates users from the database management system [18], [31]. At the final stage, the team need to carry out the task of Preparing Investigation Environment [63]. It makes the team capable of preparing the investigation setting in which the whole investigation task could be carried out in an effective way [23]. The investigation setting involves six different concepts: Investigation Team[64], Forensic Workstation, Found Environment, Clean Environment, Forensic Technique, and Source. The team provides the trusted forensic workstation involving the trusted forensic technique (forensic tools and methods) and the investigation sources identified formerly through the identification stage[65].

IV. CONCLUSION

The present study identified 18 identification processes derived from eighteen (18) DBF models. Then, the extracted processes were collected and refined on the basis of common objectives with the aim of identifying a common identification process model applicable to the database forensics field. It ended with proposing the Common Identification Process Model (CIPM). The identified processes and models were comprehensively investigated; based on the results obtained, CIPM showed that six stages are commonly involved in the database forensic investigation process: notifying of incident, incident responding, identifying source, verifying of incident, isolating database server, and preparing the investigation setting. Afterward, the perfectness of CIPM was confirmed with the use of the existing database forensic investigation models.

The studies conducted into this subject in future could 1) analyze the concepts and relationships that exist within each of the identified stages in CIPM through the use of a software

engineering approach that is recognized as metamodel, and 2) evaluate CIPM by means of the real-world case studies.

REFERENCES

[1] A. Al-Dhaqm, S. Abd Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," J. Teknol., vol. 78, no. 6–11, 2016.

[2] A. Al-Dhaqm et al., "Database forensic investigation process models: A review," IEEE Access, vol. 8, pp. 48477–48490, 2020.

[3] I. U. Onwuegbuzie, S. Abd Razak, I. Fauzi Isnin, T. S. J. Darwish, and A. Al-Dhaqm, "Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach," PLoS One, vol. 15, no. 8, p. e0237154, 2020.

[4] M. Ngadi, R. Al-Dhaqm, and A. Mohammed, "Detection and prevention of malicious activities on RDBMS relational database management systems," Int. J. Sci. Eng. Res., vol. 3, no. 9, pp. 1–10, 2012.

[5] S. Abd Razak, N. H. M. Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," IEEE Access, vol. 8, pp. 43256–43264, 2020.

[6] M. Bakhtiari and A. M. R. Al-dhaqm, "Mechanisms to Prevent lose Data."

[7] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," WIREs Forensic Sci., vol. 2, no. 5, pp. 1–18, 2020, doi: 10.1002/wfs2.1372.

[8] D. Ellison, H. Venter, and A. Ikuesan, "An Improved Ontology for Knowledge Management in Security and Digital Forensics," in European Conference on Cyber Warfare and Security, 2017, pp. 725--733.

[9] D. Ellison, A. R. Ikuesan, and H. Venter, "Description Logics and Axiom Formation for a Digital Forensics Ontology," in European Conference on Cyber Warfare and Security, 2019, pp. 742--XIII.

[10] D. Ellison, R. A. Ikuesan, and H. S. Venter, "Ontology for Reactive Techniques in Digital Forensics," 2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019, pp. 83–88, 2019, doi: 10.1109/AINS47559.2019.8968696.

[11] A. Al-Dhaqm et al., "Categorization and organization of database forensic investigation processes," IEEE Access, vol. 8, pp. 112846–112858, 2020.

[12] A. Al-Dhaqm et al., "CDBFIP: Common database forensic investigation processes for Internet of Things," IEEE Access, vol. 5, pp. 24401–24416, 2017.

[13] A. Ali, S. Abd Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," PLoS One, vol. 12, no. 4, p. e0176223, 2017.

[14] A. M. R. Al-Dhaqm, S. H. Othman, S. Abd Razak, and A. Ngadi, "Towards adapting metamodelling technique for database forensics investigation domain," in 2014 International Symposium on Biometrics and Security Technologies (ISBAST), 2014, pp. 322–327.

[15] A. Aldhaqm, S. Abd Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual investigation process model for managing database forensic investigation knowledge," Res. J. Appl. Sci. Eng. Technol., vol. 12, no. 4, pp. 386–394, 2016.

[16] V. R. Kebande, R. A. Ikuesan, N. M. Karie, S. Alawadi, K.-K. R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," Forensic Sci. Int. Reports, vol. 2, p. 100122, 2020.

[17] A. Al-dhaqm, M. Bakhtiari, E. Alobaidi, and A. Saleh, "Studding and Analyzing Wireless Networks Access points."

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

[19] A. Ali, A. Al-Dhaqm, and S. A. Razak, "Detecting Threats in Network Security by Analyzing Network Packets using Wireshark," 2014.

[20] K. Fowler, G. Gold, and M. Mcsd, "A real world scenario of a SQL Server 2005 database forensics investigation," Inf. Secur. Read. room Pap. SANS Inst., 2007.

[21] D. Litchfield, "Oracle forensics part 4: Live response," NGSSoftware Insight Secur. Res. (NISR), Next Gener. Secur. Softw. Ltd., Sutt., 2007.

[22] V. R. Kebande and H. S. Venter, "Adding event reconstruction to a Cloud Forensic Readiness model," 2015, doi: 10.1109/ISSA.2015.7335050.

[23] K. Fowler, SQL server forenisc analysis. Pearson Education, 2008.

[24] D. Lee, J. Choi, and S. Lee, "Database forensic investigation based on table relationship analysis techniques," in 2009 2nd International Conference on Computer Science and Its Applications, CSA 2009, 2009, p. 5404235.

[25] N. Karie, V. Kebande, and H. Venter, "A generic framework for digital evidence traceability," in European Conference on Information Warfare and Security, ECCWS, 2016, vol. 2016-Janua.

[26] 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 FTRA International Conference on Secure and Trust Computing, Data Management, and Application, 2011, pp. 164–171.

[27] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," Aust. J. Forensic Sci., vol. 50, no. 5, 2018, doi: 10.1080/00450618.2016.1267797.

[28] V. R. Kebande and H. S. Venter, "On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges," Aust. J. Forensic Sci., vol. 50, no. 2, 2018, doi: 10.1080/00450618.2016.1194473.

[29] S. Tripathi and B. B. Meshram, "Digital evidence for database tamper detection," 2012.

[30] H. K. Khanuja and D. S. Adane, "A framework for database forensic analysis," Comput. Sci. Eng. An Int. J., vol. 2, no. 3, pp. 27–41, 2012.

[31] R. Susaimanickam, "A workflow to support forensic database analysis." Murdoch University, 2012.

[32] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, "Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes," 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 200–205, 2020, doi: 10.1109/ICIoT48696.2020.9089494.

[33] O. M. Fasan and M. S. Olivier, "On Dimensions of Reconstruction in Database Forensics.," in WDFIA, 2012, pp. 97–106.

[34] H. Beyers, M. S. Olivier, and G. P. Hancke, "Arguments and Methods for Database Data Model Forensics.," in WDFIA, 2012, pp. 139–149.

[35] 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." University of Nairobi, 2016.

[36] T. Hungwe, H. S. Venter, and V. R. Kebande, "Scenario-Based Digital Forensic Investigation of Compromised MySQL Database," 2019, doi: 10.23919/ISTAFRICA.2019.8764819.

[37] B. Zawali, R. A. Ikuesan, V. R. Kebande, S. Furnell, and A. A-Dhaqm, "Realising a Push Button Modality for Video-Based Forensics," Infrastructures, vol. 6, no. 4, p. 54, 2021, doi: 10.3390/infrastructures6040054.

[38] A. R. Ikuesan and H. S. Venter, "Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet?," Digit. Investig., vol. 30, pp. 73–89, 2019.

[39] J. Whittle, "Workshops and Tutorials at the UML 2002 Conference," in International Conference on the Unified Modeling Language, 2002, pp. 442–447.

[40] A. Aldhaqm, S. Abd Razak, and S. H. Othman, "Common Investigation Process Model for Database Forensic Investiga-tion Discipline," in the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia, 2015, pp. 297–300.

[41] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. Ali Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," PLoS One, vol. 12, no. 2, p. e0170793, 2017.

[42] I. Kigwana, V. R. Kebande, and H. S. Venter, "Towards an e-government framework for the Republic of Uganda," 2017, doi: 10.23919/ISTAFRICA.2017.8101971.

[43] V. Kebande and H. Venter, "Towards a model for characterizing potential digital evidence in the cloud environment during digital forensic readiness process," in Proceedings of the International Conference on Cloud Security Management, ICCSM, 2015, vol. 2015-Janua.

[44] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Towards adapting metamodeling approach for the mobile forensics investigation domain," in International Conference on Innovation in Science and Technology (lICIST), 2015, p. 5.

[45] J. Choi, K. Choi, and S. Lee, "Evidence investigation methodologies for detecting financial fraud based on forensic accounting," in 2009 2nd International Conference on Computer Science and Its Applications, CSA 2009, 2009, p. 5404202.

[46] M. S. Olivier, "On metadata context in database forensics," Digit. Investig., vol. 5, no. 3–4, pp. 115–123, 2009.

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

[48] H. Q. Beyers, "Database forensics: Investigating compromised database management systems." University of Pretoria, 2013.

[49] H. Khanuja and S. S. Suratkar, "Role of metadata in forensic analysis of database attacks," in 2014 IEEE International Advance Computing Conference (IACC), 2014, pp. 457–462.

[50] 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. Investig., vol. 11, no. 4, pp. 336–348, 2014.

[51] O. M. Adedayo and M. S. Olivier, "Ideal log setting for database forensics reconstruction," Digit. Investig., vol. 12, pp. 27–40, 2015.

[52] J. Wagner, A. Rasin, and J. Grier, "Database forensic analysis through internal structure carving," Digit. Investig., vol. 14, pp. S106–S115, 2015.

[53] V. R. Kebande and R. A. Ikuesan, "Virtual sensor forensics," 2020, doi: 10.1145/3415088.3415117.

[54] 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), 2018, pp. 75–80.

[55] 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, doi: 10.1109/ACCESS.2020.3008696.

[56] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping process of digital forensic investigation framework," Int. J. Comput. Sci. Netw. Secur., vol. 8, no. 10, pp. 163–169, 2008.

[57] A. Ali, S. Abd Razak, S. H. Othman, and A. Mohammed, "Extraction of common concepts for the mobile forensics domain," in International Conference of Reliable Information and Communication Technology, 2017, pp. 141–154.

[58] C. M. Macal, "Model verification and validation," 2005.

[59] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," 2016, doi: 10.1109/FiCloud.2016.57.

[60] V. R. Kebande, N. M.Karie, and H. S. Venter, "Functional requirements for adding digital forensic readiness as a security component in IoT environments," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 2, 2018, doi: 10.18517/ijaseit.8.2.2121.

[61] V. R. Kebande and H. S. Venter, "CFRaaS: Architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent," African J. Sci. Technol. Innov. Dev., vol. 11, no. 6, pp. 749–769, 2019, doi: 10.1080/20421338.2019.1585675.

[62] V. R. Kebande and H. S. Venter, "A comparative analysis of digital forensic readiness models using CFRaaS as a baseline," Wiley Interdiscip. Rev. Forensic Sci., vol. 1, no. 6, pp. 1–12, 2019, doi: 10.1002/wfs2.1350.

[63] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R. Kebande, and S. H. Othman, "Face validation of database forensic investigation metamodel," Infrastructures, vol. 6, no. 2, 2021, doi: 10.3390/infrastructures6020013.

[64] A. Al-Dhaqm, S. Abd Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," IEEE Access, vol. 8, pp. 173359–173375, 2020.

[65] V. R. Kebande, P. Mudau, R. A. Ikuesan, H. S. Venter, and K.-K. R. Choo, "Holistic Digital Forensic Readiness Framework for IoT-Enabled Organizations," Forensic Sci. Int. Reports, p. 100117, 2020, doi: https://doi.org/10.1016/j.fsir.2020.100117.