Journal of Computer Science

Original Research Paper

Reconstruction Investigation Model for Database Management Systems

Abdulaziz Saleh Alraddadi

College of Computer Science and Engineering, Taibah University Yanbu, Saudi Arabia

Article history
Received: 31-07-2023
Revised: 24-10-2023
Accepted: 25-10-2023

Email: alraddadi1@yahoo.com

Abstract: There have been increased levels of cybercrime in the database industry, which has hurt the confidentiality, integrity, and availability of these systems. Most organizations apply several security layers to detect and prevent database crimes. For this reason, Database Forensics (DBF) plays a very important role in capturing and discovering, who the criminal is, when the crime was committed, and which part of the database the crime occurred. Several forensic models have been proposed for the DBF field, which can be used to identify, collect, preserve, examine, analyze, and document database crimes. However, most of these models focused on specific database systems due to the variety of the database infrastructure and the multidimensional nature of the database systems. The most important part of the DBF field is the analysis process used to investigate the captured data and discover the attack. Thus, this study proposes an Integrated Reconstruction Investigation Model (IRIM) for database forensics using a metamodeling method. It consists of two main processes: The examining process and the discovering and reporting process. A real scenario has been used to validate the effectiveness of the proposed model. According to the results, the proposed model could detect database cybercrimes and allow domain forensic practitioners to capture and analyze database crimes efficiently.

Keywords: Design Science Research Database Forensics, Database Systems, Reconstruction Process, Investigation Model

Introduction

The field of digital forensics has evolved over the past few years to address the challenges posed by cybercrimes, cybersecurity threats, and the protection of digital data in our increasingly digital age. As a result of using advanced techniques, tools, and methods, digital forensics experts can solve crimes, strengthen cybersecurity, and provide valuable evidence during legal proceedings. There are several challenges that the field of digital forensics faces, including data overload, encryption, the rapid development of technologies, and legal considerations, which necessitate continued innovation and expertise in this field.

On the other hand, the field of cyber security is one of the most crucial areas for protecting sensitive information (Al-Dhaqm *et al*., 2023a; Alotaibi *et al*., 2023a). Security techniques, models, frameworks, procedures, policies, and processes have been proposed in several fields. These include database systems (Al-Dhaqm *et al*., 2023b), networks, robotics (Mohammed *et al*., 2021), prevent cyberbullying (Yafooz *et al*., 2023), wireless networks (Onwuegbuzie *et al*., 2022; Al-dhaqm *et al*., 2013) cloud security (Al-Mugerrn *et al*., 2023; Zubair *et al*., 2022), the internet of vehicles, IoT (Saleh *et al*., 2023), UAV field and mobile field (Yahya *et al*., 2023), medical field (Qureshi *et al*., 2022; Ngadi *et al*., 2012; Onwuegbuzie *et al*., 2020; Abd Razak *et al*., 2020; Altowayti *et al*., 2022; Rasool *et al*., 2022; Mohammed *et al*., 2022; Onwuegbuzie *et al*., 2021; Bakhtiari and Al-dhaqm, 2012).

Database crimes increase daily, threatening privacy, integrity, and accessibility (Al-Dhaqm *et al*., 2023b). It is therefore essential to have a database forensics field that investigates who is the criminal when the crimes occur, and how they occurred (Salem *et al*., 2023). The purpose of database forensic investigations is to obtain digital evidence primarily from the target database for analysis, preservation, reconstruction, and presentation as evidence during subsequent litigation proceedings (Alfadli *et al*., 2021; Zawali *et al*., 2021; Al-Dhaqm *et al*., 2015; Alhussan *et al*., 2022a). In most cases, the evidence can be used to develop a hypothesis which can then be presented as evidence that can be used as a basis for litigation (Alotaibi *et al*., 2022b). As a specialty field of

digital forensics, database forensics offers the opportunity to employ scientifically prescribed methods for the identification, collection, preservation, reconstruction, analysis, and documentation of database incidents (Al-Dhaqm *et al*., 2020a; Alotaibi *et al*., 2022a). In spite of this, database forensics is still seen as a complex, ambiguous, and heterogeneous area due to the fact that database systems are considered to be multifaceted (Al-Dhaqm *et al*., 2020b).

Thus, database forensic investigation is the process of investigating and analyzing databases as part of forensic science principles and techniques to uncover evidence pertaining to cybercrime or other illegal activities by utilizing forensic science principles and techniques (Al-Dhaqm *et al*., 2020a). An analysis of a database involves the examination and retrieval of data from a database, as well as the identification and analysis of any potential security breaches and unauthorized access to that database (Al-Dhaqm *et al*., 2017a). Due to the increasing reliance on databases to store and manage sensitive information in our society, the field of database forensics has gained significant importance in recent years. Many industries, across a variety of sectors, use databases to store data, including customer records, financial transactions, and personal information, and thus database services are very common across them (Frühwirt *et al*., 2013; Alotaibi *et al*., 2023b). As a result of database forensics, the objective is to identify and collect evidence that will be useful to the legal process or internal investigations that may require evidence. An example of this type of evidence could be deleted or altered records, log files, access logs, and other digital artifacts that may provide insight into the actions of an individual or group involved in illegal activities that can provide evidence of their involvement.

Due to the complexity and heterogeneity of database systems, specific and redundant collection and analysis models in the database forensic field are considered redundant. This study explores the need for identifying an integrated model that focuses on examining and analyzing. This is a step toward reducing redundancy. The authors have proposed an Integrated Reconstruction Investigation Model for the database forensic field, herein called IRIM. This model is evaluated based on a real scenario. The metamodeling method was adapted for development and validation (Al-Dhaqm *et al*., 2020c). Using metamodels or response surface models, one can create surrogate models in modeling and simulation. Models such as these approximate the behavior of complex systems or processes. As part of this study, the FTK Imager and Hash my files forensic tools have been applied to solve the problem related to a database attack scenario. FTK Imager is open-source software developed to access data that can be used to perform many criminal analysis functions (Utomo *et al*., 2023). Hash my files is a small utility that allows you to calculate the MD5 and SHA1 hashes of a file or files with the click of a button (Aderibigbe and Chi, 2017).

The proposed IRIM is intended to be used to reconstruct database events or incidents based on the available evidence in a database. It is a process where different techniques, methodologies, and expertise are combined, to construct a comprehensive picture of what occurred.

The purpose of this section is to discuss existing digital forensic works and to focus on the models that have been proposed in the literature for the examination and reconstruction of database process models. Several forensic examinations and reconstruction models have been proposed for the database systems. For example, the authors Wong and Edwards (2005) proposed a reconstruction model to rebuild intruder activities by showing malicious actions to reconstruct a database. In this way, the database was able to be restored. The research conducted by Fowler *et al*. (2007) has also suggested that part of the suggested model includes media analysis, data recovery, timeline creation, and string search processes as part of its implementation. Additionally, Fowler (2008) stated that this is part of the artifact analysis process that is utilized when analyzing malicious activity and retracing events that occurred in the past. However, (Choi *et al*., 2009) referred to that analysis process as a business and financial data analysis, using it to uncover fraudulent transactions that had taken place. There are other models that describe the analysis process as one of restoration and searchability (Onwuegbuzie *et al*., 2022), where research by Al-Dhaqm *et al*. (2013) essentially, this is the process of investigating how the data collection process was conducted. Furthermore, research by Khanuja and Adane (2012); implicitly describes this as a part of the reconstruction process and the physical and digital examination process. Also, Adedayo and Olivier (2015) proposed the forensic analysis process, which uses log management or log analysis tools to enhance the information volume analysis retrieved from log files in database forensics. In other models, the reconstruction and analysis process was described as an analysis of database attacks and analysis of anti-forensic attacks (Khanuja and Suratkar, 2014), reconstructing evidence (Frühwirt *et al*., 2014), forensic analysis (Khanuja and Adane, 2013) and rebuilding volatile artifacts (Wagner *et al*., 2015).

Additionally, Chopade and Pachghare (2019) proposed a survey study, which concentrated on the latest research on forensic examination of RDBMS and NoSQL databases and the survey of artifacts to be studied for database forensics. A prototype developed by Orosco *et al*. (2020) focuses on analyzing the possibility of rebuilding database contents from the Redo logs of a MySQL DBMS and gathering related data from the redo log files. Another research by Adamu *et al*. (2020) provided a study on the database anti-forensics agents and the bad effects at numerous phases of the database forensics processes. In

addition, Marsh *et al*. (2019) proposed a model to perform a deep forensic examination of HarperDB using a grouping of two methods: Database Forensics (DBF) which presents related stages to perform database forensic investigation, and common database forensic investigation process specifying appropriate stages to examine IoT environments.

Also, research by Al-Dhaqm *et al*. (2021a) also offers a face validation approach for the Database Forensics Metamodel (Bakhtiari and Al-dhaqm, 2012), used to evaluate the completeness, logicalness, and usefulness of the database forensics domain. Other research includes (Choi *et al*., 2021) which offered a recovery model to retrieve deleted information from MSSQL.

The authors of the article (Al-Dhaqm *et al*., 2017a) have proposed a common process for database forensic investigation based on design science research. The proposed process is divided into four phases: Identification; collecting the artefacts; analysing the artefacts; and documenting and presenting the results (Abd Razak *et al*., 2016). Using a metamodeling approach, the researchers in Al-Dhaqm *et al*. (2017b; 2014) attempted to integrate existing attempts to represent database forensic knowledge in a reusable form while providing a single viewpoint from which to look at database access. According to the authors in Al-Dhaqm *et al*. (2020d), a harmonized mobile forensic investigation process model for the mobile forensic field goes a long way towards incorporating and streamlining the whole redundant investigation process within the mobile forensic sector. A metamodel for the mobile forensic domain has been proposed by Ali *et al*. (2015; 2017; 2018). According to the authors in Ali *et al*. (2017); Kebande *et al*. (2020), a metamodeling approach has been developed for mobile forensics, wherein common concepts that pertain to mobile forensics were identified.

A generic process model for database forensic investigation was presented by Al-Dhaqm *et al*. (2016). The process involves identifying, collecting, preserving, analyzing, and presenting the evidence collected during a forensic investigation. Using the developed model, the concepts and terminologies of all common database forensic investigations can be reconciled (Al-Dhaqm *et al*., 2021b). In order to facilitate the management of domain knowledge among practitioners, (Al-Dhaqm *et al*., 2018; Alhussan *et al*., 2022b) proposed a model-driven database forensic investigation system called model-driven database forensic investigation system. Table 1 displays the advantages and disadvantages of the existing database forensics models.

Table 1: Description of the excusing database forensics models

No.	Ref.	Description
1.	Wong and Edwards (2005)	As presented in this study, the author proposed a reconstruction mechanism to reconstruct an intruder's activities by demonstrating malicious actions that can be used to reconstruct a database. As a result, it would be possible to restore the database in this manner
2.	Fowler *et al*. (2007)	In accordance with the researchers' findings, the implemented model would be accompanied by processes such as media analysis, data recovery, timeline creation, and string search process to accomplish its goals
3.	Fowler (2008)	As it appears, this procedure is a part of the artifact analysis process that is used to analyze malicious activity and retrace previously occurred events in order to identify perpetrators
4.	Choi *et al*. (2009)	To uncover fraudulent transactions that had taken place, the company engaged in what it called a business and financial data analysis in order to uncover potential frauds
5.	Khanuja and Adane (2012)	There is a framework proposed in this research paper that enables the analysis and reconstruction of the the activity of any unsuspected behavior within a database to be performed. There is a purpose for identifying , collecting, analyzing, validating, interpreting, generating forensic reports, and preserving the evidence for digital investigations in order to conduct a forensic investigation
6.	Adedayo and Olivier (2015)	proposed the forensic analysis process, which uses log management or log analysis tools to enhance the information volume analysis retrieved from log files in database forensics
7.	Adedayo and Olivier (2015)	In this study, the authors present the notion of an ideal log setting to facilitate the successful reconstruction of databases for the purpose of forensic analysis. Several of the most popular database management systems have been compared with their default preferences for database management systems in this study. Furthermore, for a database log to be useful during the reconstruction process, it is necessary to identify what information must be logged in that log
8.	Khanuja and Suratkar (2014)	This study focuses on the importance of metadata for database forensics and its significance in this study. In accordance with their proposal, they developed a system that enables forensic analysis of databases to be performed independent of the database management system used in order to generate metadata files
9.	Frühwirt *et al*. (2014)	In this study, a novel approach was presented that utilizes transaction and replication sources to build a forensic -aware database management system. In order to reconstruct evidence during a forensic investigation, the team relied on internal data structures as a baseline for the evidence
10.	Khanuja and Adane (2013)	An extensive study of database forensics has been carried out by the authors of this study and they have proposed a methodology for collecting and analyzing evidence and artifacts (volatile and non-volatile) such as data caches, log files, and so on
11.	Wagner *et al*. (2015)	As part of their research, the authors have developed an academic tool that supports a wide range of databases seamlessly, rebuilding data content such as tables from any leftover fragment of storage on disk or in memory that remains. This study proposes an automatic method of reverse engineering storage in a new database (with a minimum amount of user intervention) in order to detect volatile data changes and identify user action artifacts that might exist

As a result of this comprehensive review of all database forensic models, it becomes evident that the database forensic domain lacks an integrated reconstruction model that can be used to reconstruct and investigate database crimes using a database forensic investigation.

Materials and Methods

The purpose of this study is to develop and validate the IRIM by using a metamodeling approach (Al-Dhaqm *et al*., 2017a). By using metamodeling, you have the ability to integrate and define models from a variety of domains (Geisler *et al*., 1998). As a result, it is possible to identify and share common processes between these different viewpoints. Therefore, metamodeling can be applied successfully in a very wide range of different application domains, especially for standardization purposes. Basically, metamodeling describes the process of identifying the general processes that exist within a given problem domain and the relationships between them. In the current domain, it is used for the solving of complex, interoperable, and heterogeneous issues (Whittle, 2002) as a result, metamodels should be formally defined thoroughly in addition to being well-structured. Therefore, the methodology consists of five stages as shown in Fig. 1. (1) Collecting DBF examination and reconstruction models, (2) Extracting common processes (3) Combining common processes, (4) Proposing an IRIM model and (5) Evaluating the proposed IRIM model.

DBF examination and analysis models are collected in the first stage and common examination and analysis processes are extracted in the second stage. In stage three, processes that have similar names and meanings or different names with similar meanings are combined into one process. As a result of stage 3, we are able to propose the IRIM model based on the output of the third stage. The effectiveness and capabilities of the proposed IRIM will be evaluated in the final stage. Table 2 displays extracted processes from the collected models. Figure 2 displays the proposed IFIM. The proposed IRIM consists of two main processes: The examination process and, the discovering and reporting process:

1. Examination process: The purpose of this process is to check the authenticity of the data captured during the capture process. This process is used after the acquisition and preservation processes have been completed. By using the proper forensic tools, the investigation team acquires and preserves the volatile and non-volatile data from the relevant resources to solve the case. As a result, the investigation team will rehash the hashed values of the captured data and verify the authenticity of the captured data by rehashing the hashed values. If the data is authentic, the investigation team will move on to the next step in the investigation process, otherwise, it will make another copy of the original data
2. Discovering and reporting process: The purpose of this process is to find and report any database crimes that may have occurred. It is important for the investigation team to assign suitable keywords that can be used to help find matching patterns of database crimes that may assist with the investigation. An investigation team should attempt this process several times until they find the evidence of the database crime, which is an iterative process that involves trying a variety of keywords until they find the evidence of the database crime. If the investigation team finds evidence, they will compile and organize the evidence into a report that will be documented as effectively as possible

Table 2: Extracted processes from the collected models

No.	Similar processes	References
12.	Reconstructing database	Wong and Edwards (2005)
13.	Restoring database integrity	Wong and Edwards (2005)
14.	Media analysis	Fowler *et al*. (2007)
15.	Timeline creation	Fowler *et al*. (2007)
16.	Data recovery	Fowler *et al*. (2007)
17.	Search string	Fowler *et al*. (2007)
18.	Artifact analysis	Fowler (2008)
19.	Economic and commercial data analysis	Choi *et al*. (2009)
20.	Rebuilding and search ability	Olivier (2009)
21.	Examination of data composed	Son *et al*. (2011)
22.	Artifact investigation	Khanuja and Adane (2012)
23.	Rebuilding	Susaimanickam (2012)
24.	Reconstruction of the database	Adedayo and Olivier (2015)
25.	Forensic analysis	Khanuja and Adane (2013)
26.	Study anti-forensic crimes, examination database crimes	Khanuja and Suratkar (2014)
27.	Rebuilding evidence	Frühwirt *et al*. (2014)
28.	Rebuilding process	Khanuja and Adane (2013)
29.	Recreating volatile artifacts	Wagner *et al*. (2015)
30.	Recovering database schema	Orosco *et al*. (2022)
31.	Examination stage	Marsh *et al*. (2019)

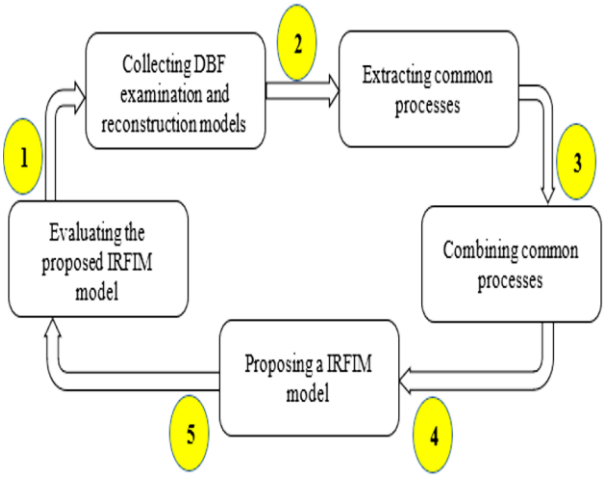

Fig. 1: Metamodeling approach (Al-Dhaqm *et al*., 2017a)

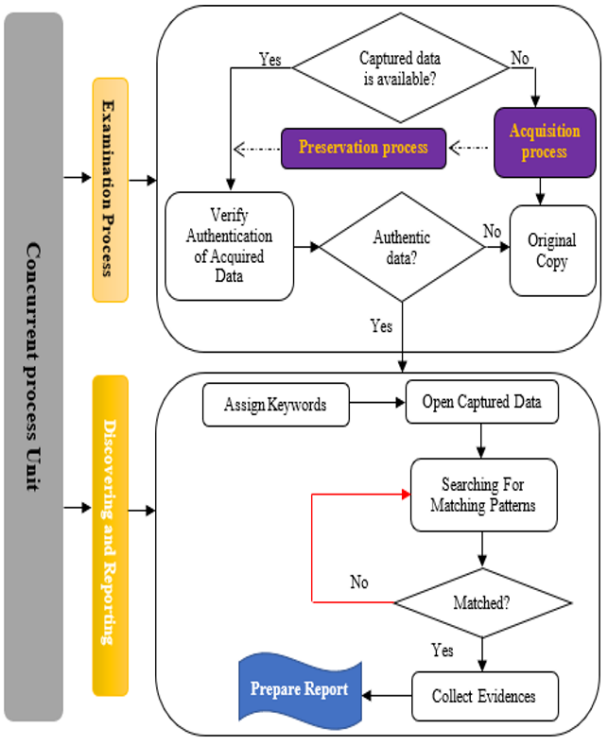

Fig. 2: Integrated reconstruction investigation model for database systems

Implementation

The purpose of this section is to demonstrate the suitability of the proposed IRIM to verify and analyze crimes committed against the database. For this purpose, the authors prepared a scenario as shown in Fig. 3. The authors assumed that the attacker compromised the account of a customer, inserted SQL injection into the customer table, updated the secret key column, and prevented the customer from making an online purchase through the website. In the next few paragraphs, we shall describe in detail the capabilities of the proposed IRIM as it relates to examining and verifying database incidents:

a) Examination process: A preliminary investigation of this case showed that, in accordance with the above scenario, there had been a compromise in the customer table. It appears that some customers' records were duplicated by an anonymous attacker, as can be seen in Fig. 4. There has been a hacking attempt on the account of the customer named "Fahad", who has the customer_ID 121356 and a duplicate record has been created for his account by the attacker

According to the initial analysis in Fig. 5, a comprehensive investigation was conducted by the investigation team using FTK images to capture the entire volatile data from the RAM. Figure 6 displays the captured data gathered from the RAM. Sequentially, the gathered data has been preserved using the hash my file tool as shown in Fig. 7. The hash my file tool produced a unique hash value for the captured data. Meanwhile, to verify the authenticity of the captured data for analysis, the FTK Imager was used to verify the hashed image that had previously been hashed. According to Fig. 8, the results of the verification showed that the captured data had the same value as the hash value of Fig. 7, which indicates that the data is original and has not been altered. As a result, the main objective of the examination process of the IRIM has been achieved successfully:

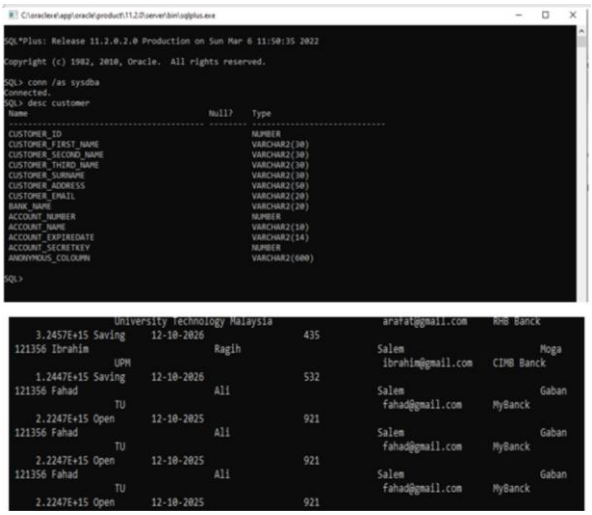

Fig. 3: Scenario of database attack

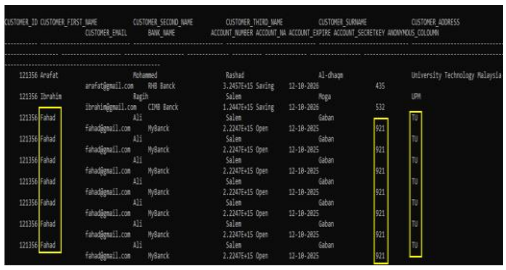

Fig. 4: Duplicated customers' records

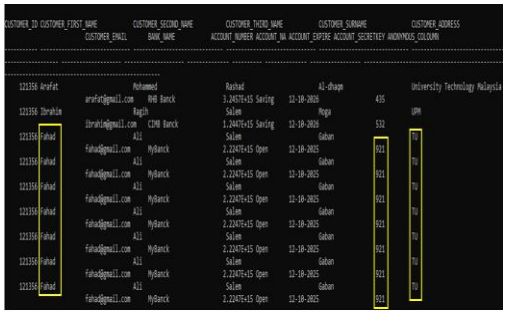

Fig. 5: Initial investigation

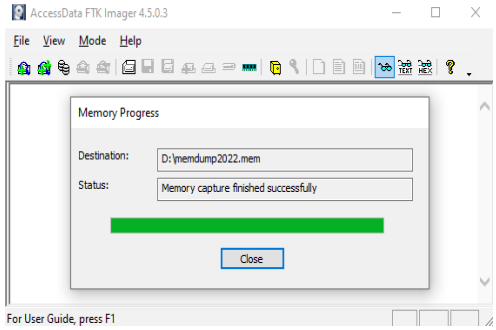

Fig. 6: Captured data from RAM using FTK imager tool

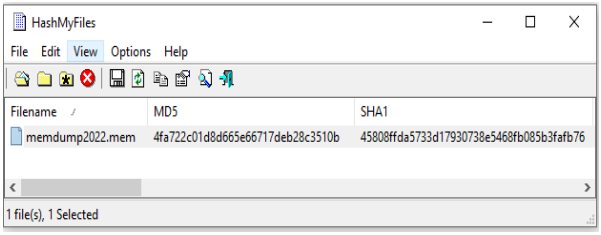

Fig. 7: Preserve captured data using the Hash my files tool

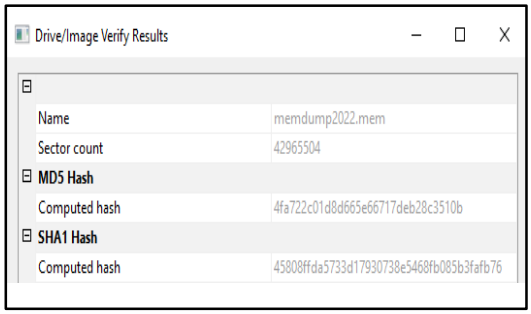

Fig. 8: The authenticity of the captured data is verified

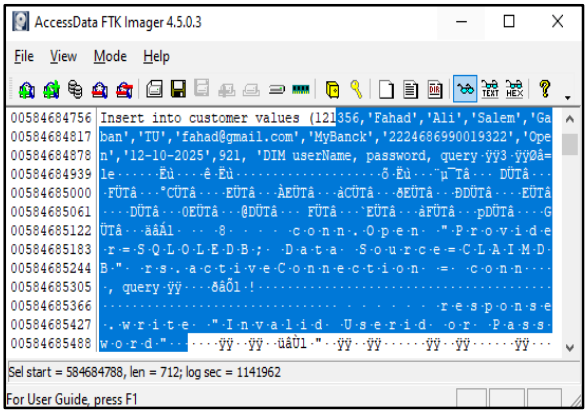

Fig. 9: Analysing the database crime

b) Discovering and reporting process: In this stage, the clean data will be analyzed, the database incidents will be discovered and a report will be prepared for the entire investigation. Using the FTK Imager, the authors open the cleaned and captured image for analysis as shown in Fig. 8. Several patterns were tried by the authors to discover how the attacker acted. Therefore, the authors were able to detect the malicious activities that were being used by the attacker because of the analysis. Figure 9, we can see the types of evidence that point to this type of crime being committed. An investigation team should prepare a comprehensive report after discovering the database crimes committed by the attacker

Results and Discussion

In this section, we discuss the results of the study. The literature has proposed several models and frameworks for the study of database forensics, each of which discusses DBFs from a different perspective. This study discusses the DBFs from the reconstruction perspective and proposes an integrated reconstruction and investigation model based on a metamodeling approach. Basically, it consists of two processes: Examination and discovery, as well as reporting processes. We have validated the proposed model using a real scenario based on the data that we have collected. Based on the results of the study, the proposed model could be used to detect database cybercrimes and permit domain forensic practitioners to capture and analyze database crimes more efficiently.

In this study, FTK Imager was used as a forensic tool in order to investigate and analyse database crimes as part of an investigation and investigation process.

Table 3: Comparing the proposed IRIM with existing database reconstruction models

No.	Existing processes	Ref.	Proposed IRIM	Status
1.	Reconstructing database	Wong and Edwards (2005)	☑	Covered
2.	Restoring database integrity	Wong and Edwards (2005)	☑	Covered
3.	Media analysis	Fowler *et al*. (2007)	☑	Covered
4.	Timeline creation	Fowler *et al*. (2007)	☑	Covered
5.	Data recovery	Fowler *et al*. (2007)	☑	Covered
6.	Search string	Fowler *et al*. (2007)	☑	Covered
7.	Artifact analysis	Fowler (2008)	☑	Covered
8.	Economic and commercial data analysis	Choi *et al*. (2009)	☑	Covered
9.	Rebuilding and search ability	Olivier (2009)	☑	Covered
10.	Examination of data composed	Son *et al*. (2011)	☑	Covered
11.	Artifact investigation	Khanuja and Adane (2012)	☑	Covered
12.	Rebuilding	Susaimanickam (2012)	☑	Covered
13.	Reconstruction of the database	Adedayo and Olivier (2015)	☑	Covered
14.	Forensic Analysis	Khanuja and Adane (2013)	☑	Covered
15.	Study anti-forensic crimes, examination database crimes	Khanuja and Suratkar (2014)	☑	Covered
16.	Rebuilding evidence	Frühwirt *et al*. (2014)	☑	Covered
17.	Rebuilding process	Khanuja and Adane (2013)	☑	Covered
18.	Recreating volatile artifacts	Wagner *et al*. (2015)	☑	Covered
19.	Recovering database schema	Orosco *et al*. (2020)	☑	Covered
20.	Examination stage	Marsh *et al.* (2019)	☑	Covered

In order to unravel the complexity of crimes that were committed during this time period, the use of this tool, which can perform forensic image analysis, extract data, and perform in-depth analyses, has proven to be invaluable in unravelling the complexity of the crimes that were committed during that time period. A high level of effectiveness and reliability have been shown to be associated with the FTK Imager tool and proposed model in terms of detecting database-related criminal activities based on the findings of this research.

Comparing the proposed IRIM with the existing DBF models shown in Table 3, the proposed IRIM is compatible with the existing models and covers the majority of them as well. For example, Wong and Edwards (2005) proposed two processes that can be used to restore the integrity of the database, namely reconstructing the database, and restoring its integrity. It was proposed by Fowler *et al*. (2007) that four processes could be employed: Media analysis, timeline creation, data recovery, and search string extraction. A summary of the proposed processes by different authors can be found in Table 3. There is no doubt that all these models are covered by the proposed IRIM.

Conclusion

It is widely believed that database forensics is one of the most important fields in the use of capturing and analyzing data that comes from databases and this is the purpose of database forensics. As a result, this field is vital when it comes to investigating, discovering, and reconstructing events related to databases. There are several forensic techniques and methodologies that are applied to the investigation, detection, and reconstruction of events related to databases, through the application of forensic techniques and methodologies. Several reconstruction models and frameworks have been proposed in the literature for database systems. Nevertheless, most of these models focused on a specific database system because of the variety of database infrastructures available and the multidimensional nature of the database systems. In this study, an integrated reconstruction investigation model for the database system called the Integrated Reconstruction Investigation Model, is proposed. This model consists of two main processes: The examination process and the recovery and reporting process. The proposed model has been evaluated using real scenarios and the results showed that the IRIM is a powerful tool that can be used to verify and analyze database crimes effectively in an accurate and efficient manner. The future work of this study will be to validate the completeness of the proposed IRIM by comparing it with other models.

Acknowledgment

I would like to express my deepest gratitude to the researchers who supported this study with all the necessary references.

Funding Information

For this research, there have been no funds available.

Ethics

By signing this document, I certify that this article has not been published anywhere else in the world.

References

Abd Razak, S., Nazari, N. H. M., & Al-Dhaqm, A. (2020). Data anonymization using pseudonym system to preserve data privacy. *IEEE Access*, *8*, 43256-43264. https://doi.org/10.1109/ACCESS.2020.2977117

Abd Razak, S., Othman, S. H., Aldolah, A. A., & Ngadi, M. A. (2016). Conceptual investigation process model for managing database forensic investigation knowledge. *Research Journal of Applied Sciences, Engineering and Technology*, *12*(4), 386-394. https://doi.org/10.19026/rjaset.12.2377

Adamu, B. Z., Karabatak, M., & Ertam, F. (2020, June). A conceptual framework for database anti-forensics impact mitigation. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISDFS49300.2020.9116375

Adedayo, O. M., & Olivier, M. S. (2015). Ideal log setting for database forensics reconstruction. *Digital Investigation*, *12*, 27-40. https://doi.org/10.1016/j.diin.2014.12.002

Aderibigbe, T., & Chi, H. (2017, April). Implement Hands-on Labs for File Integrity via Open Sources. In *Proceedings of the South East Conference* (pp. 265-267). https://doi.org/10.1145/3077286.3077317

Altowayti, W. A. H., Shahir, S., Othman, N., Eisa, T. A. E., Yafooz, W. M., Al-Dhaqm, A., ... & Ali, A. (2022). The role of conventional methods and artificial intelligence in the wastewater treatment: A comprehensive review. *Processes*, *10*(9), 1832. https://doi.org/10.3390/pr10091832

Al-Dhaqm, A. M. R., Othman, S. H., Abd Razak, S., & Ngadi, A. (2014, August). Towards adapting metamodelling technique for database forensics investigation domain. In *2014 International Symposium on Biometrics and Security Technologies (ISBAST)* (pp. 322-327). IEEE. https://doi.org/10.1109/ISBAST.2014.7013142

Al-Dhaqm, A., Abd Razak, S., & Othman, S. H. (2015). Common Investigation Process Model for Database Forensic Investigation Discipline. In *the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia* (pp. 297-300).

Al-Dhaqm, A., Abd Razak, S., Dampier, D. A., Choo, K. K. R., Siddique, K., Ikuesan, R. A., ... & Kebande, V. R. (2020a). Categorization and organization of database forensic investigation processes. *IEEE Access*, *8*, 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

Al-Dhaqm, A., Abd Razak, S., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020b). Towards the development of an integrated incident response model for database forensic investigation field. *IEEE Access*, *8*, 145018-145032. https://doi.org/10.1109/ACCESS.2020.3008696

Al-Dhaqm, A., Abd Razak, S., Othman, S. H., Ali, A., Ghaleb, F. A., Rosman, A. S., & Marni, N. (2020c). Database forensic investigation process models: A review. *IEEE Access*, *8*, 48477-48490. https://doi.org/10.1109/ACCESS.2020.2976885

Al-Dhaqm, A., Abd Razak, S., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020d). A review of mobile forensic investigation process models. *IEEE Access*, *8*, 173359-173375. https://doi.org/10.1109/ACCESS.2020.3014615

Al-Dhaqm, A., Bakhtiari, M., Alobaidi, E., & Saleh, A. (2013). Studding and Analyzing Wireless Networks Access points. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b985286eb4d8dd836141fd891f44a7e9b61deb47

Al-Dhaqm, A., Razak, S., Ikuesan, R. A., R. Kebande, V., & Hajar Othman, S. (2021a). Face validation of database forensic investigation metamodel. *Infrastructures*, *6*(2), 13. https://doi.org/10.3390/infrastructures6020013

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S., & Ghabban, F. M. (2021b). Research challenges and opportunities in drone forensics models. *Electronics*, *10*(13), 1519. https://doi.org/10.3390/electronics10131519

Al-Dhaqm, A., Othman, S. H., Yafooz, W. M., & Ali, A. (2023a). Review of Information Security Management Frameworks. In *Kids Cybersecurity Using Computational Intelligence Techniques* (pp. 69-80). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21199-7_5

Al-Dhaqm, A., Yafooz, W. M., Othman, S. H., & Ali, A. (2023b). Database Forensics Field and Children Crimes. In *Kids Cybersecurity Using Computational Intelligence Techniques* (pp. 81-92). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21199-7_6

Al-Dhaqm, A., Razak, S. A., Othman, S. H., Nagdi, A., & Ali, A. (2016). A generic database forensic investigation process model. *Jurnal Teknologi*, *78*(6-11), 45-57. https://doi.org/10.11113/jt.v78.9190

Al-Dhaqm, A., Razak, S., & Othman, S. H. (2018, November). Model derivation system to manage database forensic investigation domain knowledge. In *2018 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 75-80). IEEE. https://doi.org/10.1109/AINS.2018.8631468

Al-Dhaqm, A., Razak, S., Othman, S. H., Choo, K. K. R., Glisson, W. B., Ali, A., & Abrar, M. (2017a). CDBFIP: Common database forensic investigation processes for internet of things. *IEEE Access*, *5*, 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Ali Mohammed, A. (2017b). Development and validation of a database forensic metamodel (DBFM). *PloS one*, *12*(2), e0170793. https://doi.org/10.1371/journal.pone.0170793

Alfadli, I. M., Ghabban, F. M., Ameerbakhsh, O., AbuAli, A. N., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021, June). Cipm: Common identification process model for database forensics field. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 72-77). IEEE. https://doi.org/10.1109/ICSCEE50312.2021.9498014

Alhussan, A. A., Al-Dhaqm, A., Yafooz, W. M., Emara, A. H. M., Bin Abd Razak, S., & Khafaga, D. S. (2022a). A unified forensic model applicable to the database forensics field. *Electronics*, *11*(9), 1347. https://doi.org/10.3390/electronics11091347

Alhussan, A. A., Al-Dhaqm, A., Yafooz, W. M., Razak, S. B. A., Emara, A. H. M., & Khafaga, D. S. (2022b). Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics*, *11*(8), 1168. https://doi.org/10.3390/electronics11081168

Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. *PloS One*, *12*(4), e0176223. https://doi.org/10.1371/journal.pone.0176223

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

Ali, A., Razak, S. A., Othman, S. H., & Mohammed, A. (2018). Extraction of common concepts for the mobile forensics domain. In *Recent Trends in Information and Communication Technology: Proceedings of the 2nd International Conference of Reliable Information and Communication Technology (IRICT 2017)* (pp. 141-154). Springer International Publishing. https://doi.org/10.1007/978-3-319-59427-9_16

Al-Mugerrn, R., Al-Dhaqm, A., & Othman, S. H. (2023, February). A Metamodeling Approach for Structuring and Organizing Cloud Forensics Domain. In *2023 International Conference on Smart Computing and Application (ICSCA)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICSCA57840.2023.10087425

Alotaibi, F. M., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2022a). A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/8002963

Alotaibi, F. M., Al-Dhaqm, A., Al-Otaibi, Y. D., & Alsewari, A. A. (2022b). A comprehensive collection and analysis model for the drone forensics field. *Sensors*, *22*(17), 6486. https://doi.org/10.3390/s22176486

Alotaibi, F. M., Al-Dhaqm, A., Yafooz, W. M., & Al-Otaibi, Y. D. (2023a). A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field. *Applied Sciences*, *13*(17), 9703. https://doi.org/10.3390/app13179703

Alotaibi, F., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2023b). A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field. *Engineering, Technology & Applied Science Research*, *13*(5), 11608-11615. https://doi.org/10.48084/etasr.6195

Bakhtiari, M., & Al-dhaqm, A. M. R. (2012). Mechanisms to Prevent lose Data. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=05440cc2c5ead1b857f48cac769c4269c31c3387

Choi, H., Lee, S., & Jeong, D. (2021). Forensic recovery of SQL server database: Practical approach. *IEEE Access*, *9*, 14564-14575. https://doi.org/10.1109/ACCESS.2021.3052505

Choi, J., Choi, K., & Lee, S. (2009). Evidence investigation methodologies for detecting financial fraud based on forensic accounting. In *2009 2nd International Conference on Computer Science and Its Applications, CSA 2009* (p. 5404202). https://doi.org/10.1109/CSA.2009.5404202

Chopade, R., & Pachghare, V. K. (2019). Ten years of critical review on database forensics research. *Digital Investigation*, *29*, 180-197. https://doi.org/10.1016/j.diin.2019.04.001

Fowler, K. (2008). *SQL Server Forenisc Analysis*. Pearson Education.

Fowler, K., Gold, G. C. F. A., & Mcsd, M. (2007). A real world scenario of a SQL Server 2005 database forensics investigation. *Information Security Reading Room Paper, SANS Institute*.

Frühwirt, P., Kieseberg, P., Krombholz, K., & Weippl, E. (2014). Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations. *Digital Investigation*, *11*(4), 336-348. https://doi.org/10.1016/j.diin.2014.09.003

Frühwirt, P., Kieseberg, P., Schrittwieser, S., Huber, M., & Weippl, E. (2013). InnoDB database forensics: Enhanced reconstruction of data manipulation queries from redo logs. *Information Security Technical Report*, *17*(4), 227-238. https://doi.org/10.1016/j.istr.2013.02.003

Geisler, R., Klar, M., & Pons, C. F. (1998, September). Dimensions and dichotomy in metamodeling. In *3rd BCS-FACS Northern Formal Methods Workshop (NFM) (Ilkley, 14 a 15 de septiembre de 1998)*. https://doi.org/10.14236/ewic/NFM1998.10

Kebande, V. R., Ikuesan, R. A., Karie, N. M., Alawadi, S., Choo, K. K. R., & Al-Dhaqm, A. (2020). Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. *Forensic Science International: Reports*, *2*, 100122. https://doi.org/10.1016/j.fsir.2020.100122

Khanuja, H. K., & Adane, D. (2013). Forensic analysis of databases by combining multiple evidences. *Int. J. Comput. Technol*, *7*(3), 654-663. https://doi.org/10.24297/ijct.v7i3.3446

Khanuja, H. K., & Adane, D. S. (2012). A framework for database forensic analysis. *Computer Science & Engineering: An International Journal (CSEIJ)*, *2*(3), 27-41. https://doi.org/10.5121/cseij.2012.2303

Khanuja, H., & Suratkar, S. S. (2014, February). Role of metadata in forensic analysis of database attacks. In *2014 IEEE International Advance Computing Conference (IACC)* (pp. 457-462). IEEE. https://doi.org/10.1109/IAdCC.2014.6779367

Marsh, R., Belguith, S., & Dargahi, T. (2019, July). IoT database forensics: an investigation on HarperDB Security. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems* (pp. 1-7). https://doi.org/10.1145/3341325.3341993

Mohammed, M. Q., Kwek, L. C., Chua, S. C., Al-Dhaqm, A., Nahavandi, S., Eisa, T. A. E., ... & Alandoli, E. A. (2022). Review of learning-based robotic manipulation in cluttered environments. *Sensors*, *22*(20), 7938. https://doi.org/10.3390/s22207938

Mohammed, M. Q., Kwek, L. C., Chua, S. C., Aljaloud, A. S., Al-Dhaqm, A., Al-Mekhlafi, Z. G., & Mohammed, B. A. (2021). Deep reinforcement learning-based robotic grasping in clutter and occlusion. *Sustainability*, *13*(24), 13686. https://doi.org/10.3390/su132413686

Ngadi, M., Al-Dhaqm, R., & Mohammed, A. (2012). Detection and prevention of malicious activities on RDBMS relational database management systems. *Int. J. Sci. Eng. Res*, *3*(9), 1-10.

Olivier, M. S. (2009). On metadata context in database forensics. *Digital Investigation*, *5*(3-4), 115-123. https://doi.org/10.1016/j.diin.2008.10.001

Onwuegbuzie, I. U., Abd Razak, S., & Al-Dhaqm, A. (2021, November). Multi-Sink Load-Balancing Mechanism for Wireless Sensor Networks. In *2021 IEEE International Conference on Computing (ICOCO)* (pp. 140-145). IEEE. https://doi.org/10.1109/ICOCO53166.2021.9673578

Onwuegbuzie, I. U., Abd Razak, S., Fauzi Isnin, I., Darwish, T. S., & Al-Dhaqm, A. (2020). Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach. *PloS One*, *15*(8), e0237154. https://doi.org/10.1371/journal.pone.0237154

Onwuegbuzie, I. U., Razak, S. A., Isnin, I. F., Al-Dhaqm, A., & Anuar, N. B. (2022). Prioritized Shortest Path Computation Mechanism (PSPCM) for wireless sensor networks. *Plos One*, *17*(3), e0264683. https://doi.org/10.1371/journal.pone.0264683

Orosco, C., Varol, C., & Shashidhar, N. (2020, June). Graphically Display Database Transactions to Enhance Database Forensics. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISDFS49300.2020.9116412

Qureshi, K. N., Shahzad, L., Abdelmaboud, A., Elfadil Eisa, T. A., Alamri, B., Javed, I. T., ... & Crespi, N. (2022). A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles. *Applied Sciences*, *12*(1), 476. https://doi.org/10.3390/app12010476

Rasool, M., Ismail, N. A., Al-Dhaqm, A., Yafooz, W. M., & Alsaeedi, A. (2022). A Novel Approach for Classifying Brain Tumours Combining a SqueezeNet Model with SVM and Fine-Tuning. *Electronics*, *12*(1), 149. https://doi.org/10.3390/electronics12010149

Saleh, M., Othman, S. H., Driss, M., Al-dhaqm, A., Ali, A., Yafooz, W. M., & Emara, A. H. M. (2023). A Metamodeling Approach for IoT Forensic Investigation. *Electronics*, *12*(3), 524. https://doi.org/10.3390/electronics12030524

Salem, M., Othman, S. H., Al-Dhaqm, A., & Ali, A. (2023). Development of Metamodel for Information Security Risk Management. In *Kids Cybersecurity Using Computational Intelligence Techniques* (pp. 243-253). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21199-7_17

Son, N., Lee, K. G., Jeon, S., Chung, H., Lee, S., & Lee, C. (2011). The method of database server detection and investigation in the enterprise environment. In *Secure and Trust Computing, Data Management and Applications: 8th FIRA International Conference, STA 2011, Loutraki, Greece, June 28-30, 2011. Proceedings 8* (pp. 164-171). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22339-6_20

Susaimanickam, R. (2012). *A workflow to support forensic database analysis* (Doctoral dissertation, Murdoch University).

Utomo, D. S. I., Prayudi, Y., & Ramadhani, E. (2023). Forensic Web Analysis on The Latest Version of Whatsapp Browser. *Journal of Computer Networks, Architecture and High Performance Computing*, *5*(1), 359-367. https://doi.org/10.47709/cnahpc.v5i1.2286

Wagner, J., Rasin, A., & Grier, J. (2015). Database forensic analysis through internal structure carving. *Digital Investigation*, *14*, S106-S115. https://doi.org/10.1016/j.diin.2015.05.013

Whittle, J. (2002, September). Workshops and Tutorials at the UML 2002 Conference. In *International Conference on the Unified Modeling Language* (pp. 442-447). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45800-X_34

Wong, D., & Edwards, K. (2005). System and method for investigating a data operation performed on a database. https://patents.google.com/patent/US20050289187A1/en

Yafooz, W. M., Al-Dhaqm, A., & Alsaeedi, A. (2023). Detecting Kids Cyberbullying Using Transfer Learning Approach: Transformer Fine-Tuning Models. In *Kids Cybersecurity Using Computational Intelligence Techniques* (pp. 255-267). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21199-7_18

Yahya, A. E., Gharbi, A., Yafooz, W. M., & Al-Dhaqm, A. (2023). A Novel Hybrid Deep Learning Model for Detecting and Classifying Non-Functional Requirements of Mobile Apps Issues. *Electronics*, *12*(5), 1258. https://doi.org/10.3390/electronics12051258

Zawali, B., Ikuesan, R. A., Kebande, V. R., Furnell, S., & A-Dhaqm, A. (2021). Realising a push button modality for video-based forensics. *Infrastructures*, *6*(4), 54. https://doi.org/10.3390/infrastructures6040054

Zubair, A. A., Razak, S. A., Ngadi, M. A., Al-Dhaqm, A., Yafooz, W. M., Emara, A. H. M., ... & Al-Aqrabi, H. (2022). A cloud computing-based modified symbiotic organisms search algorithm (ai) for optimal task scheduling. *Sensors*, *22*(4), 1674. https://doi.org/10.3390/s22041674