A Forensic Framework for gathering and analyzing Database Systems using Blockchain Technology

Ahmed Omar Alzahrani
Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia
aoalzahrani@uj.edu.sa

Mahmoud Ahmad Al-Khasawneh
School of Computing, Skyline University College, University City Sharjah, 1797, Sharjah, UAE | Applied Science Research Center, Applied Science Private University, Amman, Jordan | Jadara University Research Center, Jadara University, Jordan
mahmoud@outlook.my (corresponding author)

Ala Abdulsalam Alarood
College of Computer Science and Engineering, University of Jeddah, 21959 Jeddah, Saudi Arabia
aasoleman@uj.edu.sa

Eesa Alsolami
College of Computer Science and Engineering, University of Jeddah, 21959 Jeddah, Saudi Arabia
eaalsulami@uj.edu.sa

Received: 26 February 2024 | Revised: 5 March 2024 | Accepted: 11 March 2024

ABSTRACT

A blockchain is a distributed database that contains the records of transactions that are shared among all members of a community. Most members must confirm each and every transaction in order for a fraudulent transaction to fail to occur. As a rule, once a record is created and accepted by the blockchain, it cannot be altered or deleted by anyone. This study focuses on improving the investigation task in the database forensics field by utilizing blockchain technology. To this end, a novel conceptual framework is proposed for the forensic analysis of data from database systems engaging blockchain technology. This is the first time that blockchain technology is followed in database forensics for the purpose of tracing digital evidence. The design science research method was adopted to accomplish the objectives of the present study. The findings displayed that with the developed forensics framework, the data regarding database incidents could be gathered and analyzed in a more efficient manner.

Keywords-database systems; digital forensics; database forensics; design science research; blockchain technology

I. INTRODUCTION

Database systems are software systems that are used to organize, store, retrieve, and analyze data [1]. Database systems have the function of providing an interface between the end user and the system so that the end user can create, read, update, and delete data in the database. Blockchain is a technology that uses distributed ledgers which enable the secure and transparent exchange of information without the need for a central authority to supervise the latter [2]. This is a kind of decentralized system in which a computer network records and analyzes a series of transactions in real time. Several industries, including finance, healthcare, and supply chains, have been drawn to blockchain technology because of its potential applications in these fields. Database forensics is a branch of digital forensics, which focuses on the analysis and investigation of database systems [3-6]. It involves extracting, preserving, and examining the data stored in a database system. Database forensic analysis plays a crucial role in uncovering valuable evidence and understanding the behavior of a compromised system [7, 8]. It is often implemented in cybersecurity investigations to identify and analyze malicious activities, such as malware infections, unauthorized access, and data breaches. By examining the content of database systems, investigators can uncover information that might not be accessible through traditional file system analysis.

One of the key advantages of database forensics is its ability to capture real-time data, providing insight into the state of a system at the time of an incident. This allows investigators to reconstruct events and understand the actions performed by an attacker or a malicious program [9]. Several forensic approaches have been proposed to deal with database systems and to investigate incidents from three dimensions: destroyed, compromised, and changed [11]. The concept of compromised databases has been more specifically defined as ffollows: a database is considered compromised when it has been found that components of the database management system (DBMS) have been compromised by an attacker while the database itself remains operational [10]. In a damaged database, data have been modified, deleted, or copied from the original location, but have remained in their original location. Depending on the extent of the damage inflicted, these databases may or may not be any longer operational. A modified database (external dimension) refers to the database that has been modified through normal business processes, not compromised or damaged when the event of interest occurred. However, the database has continued to function normally since the event of interest occurred [10]. However, the existing approaches have not been able to provide adequate safeguards for electronic evidence before, during, and after the incident's occurrence.

The purpose of this study is to develop a novel conceptual framework for gathering and analyzing data from database systems using blockchain technology. The proposed framework consists of two main stages: gathering data and analyzing data. The developed framework streamlines the process of extracting data from database systems, enabling practitioners to effortlessly capture and analyze them.

II. RELATED WORKS

Authors in [12] proposed an extraction process for data based on the relationships connecting columns in the tables of the database. Authors in [13] introduced a model for extracting fraud data from a database server. Following the metadata extraction process proposed in [14], the metadata of the database dimension are extracted and those who are permitted to take certain action are determined. Authors in [15] presented a data collection procedure subdivided in two stages: one stage related to selecting files and another stage with a focus on the collection of all the files. In [16], a file collection process was proposed for collecting Oracle files from specific locations and then moving them to an evidence collection server. Authors in [17], developed an artifact collection process for the collection and extraction of metadata and database files from compromised MySQL Server databases in order to collect physical and digital data. Similarly, a collection procedure was proposed in [18, 19] as a sub-process of physical and digital examination. Authors in [20] proposed the collection of non-volatile artifacts such as based processes for the collection of log transactions, log files, database files, and volatile artifacts, like undo log, data caches, and redo logs. Authors in [21] recommended a collection and preservation process so that the investigators can collect MySQL, SQL, and operating systems detailed several logs. In [22], a collection process was developed to aid in gathering evidence from the replication of sources. Authors in [23] suggested an execution process allowing investigators to use forensic procedures and tools for the creation of forensic values and then collect the metadata values of the identified target files.

The model developed in [24] reconstructed a database and restored its integrity in order to rebuild intruder activities. Authors in [25] utilized media analysis, data recovery, timeline creation, and string search processes as parts of their suggested model, while authors in [20] described their model as a part of the artifact analysis process used in the analysis of malicious activity and the reconstruction of timeline events. Authors in [13] suggested a process for financial and commercial data examination and applied it in uncovering illegal operations. Some other models have described the analysis process as restoration and searchability [14]. This was referred in [15] as the investigation on the data collection process. Furthermore, authors in [17] implicitly described the latter as a part of the reconstruction process along with the physical and digital examination procedure in [18]. Additionally, authors in [26] proposed a forensic analysis process that employed 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 processes were described as analysis database attack, analysis anti-forensic attacks [27], reconstructing evidence [23], reconstruction [26], forensic analysis [22], and reconstruction of volatile artifacts [28]. Moreover, authors in [29] conducted a survey concentrating on the latest research on forensic examination of RDBMS and NoSQL databases along with the survey of artifacts to be studied for database forensics. A prototype developed in [30] was focused on analyzing the possibility of rebuilding database contents from Redo logs of a MySQL DBMS, by gathering related data from the Redo Log files. Authors in [31] studied the database anti-forensics agents and the effects they pose at numerous phases of the database forensics processes. Authors in [32] 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 databases forensic investigation, and common database forensic investigation process, which specifies appropriate stages to examine IoT environments. In [33], a unified incident response model was recommended for conducting investigation in the database forensics field. The model consisted of three steps: pre-, during-, and post-incident response. Their model followed incident investigation rules required in ISO/IEC-based guidelines for incident investigation processes. Furthermore, the authors in [34] proposed a consistent database forensic investigation procedure adopting the design science research. Their model was able to solve the redundancy of the existing investigation processes for the field of database forensics. It was created based on three key groups, i.e. planning, preparation and pre-response; acquisition and preservation; and analysis and reconstruction. In [35], a tamper detection model was developed for the NoSQL database, which worked in forensic investigation medium to offer more relevant effects on corrupt data and to give a distinction based on doubt and actual corrupt data. Authors in [36] offered a face validation approach for the Database Forensics Metamodel [37], which was used to evaluate the completeness, logicalness, and usefulness for the database forensics domain. Authors in [38] offered a recovery model to retrieve deleted information from MSSQL.

The review presented above is summarized in Table I. The existing database forensics approaches have covered the traditional digital forensics processes previously employed. Yet, blockchain technology is not applied in database forensics.

TABLE I. DATABASE FORENSICS MODELS

Year	Ref.	Gathering and protection stage	Rebuilding and analysis stage	Documenting and presentation stage	Blockchain technology
2007	[39]	✘	✘	✘	✘
2007	[40]	✘	✘	✘	✘
2007	[41]	✘	✘	✘	✘
2007	[42]	✘	✓	✘	✘
2007	[43]	✘	✓	✘	✘
2007	[44]	✘	✓	✘	✘
2007	[45]	✘	✓	✘	✘
2007	[46]	✘	✓	✘	✘
2008	[20]	✓	✓	✓	✘
2008	[47]	✘	✓	✘	✘
2006	[48]	✘	✓	✘	✘
2009	[14]	✘	✓	✘	✘
2009	[12]	✘	✓	✘	✘
2010	[49]	✘	✓	✘	✘
2011	[50]	✘	✘	✘	✘
2011	[51]	✘	✘	✘	✘
2011	[15]	✘	✘	✘	✘
2011	[52]	✘	✘	✘	✘
2012	[16]	✘	✓	✘	✘
2012	[17]	✓	✓	✓	✘
2012	[18]	✓	✓	✓	✘
2012	[53]	✘	✘	✘	✘
2012	[54]	✘	✓	✘	✘
2012	[55]	✘	✓	✘	✘
2012	[56]	✘	✓	✘	✘
2012	[57]	✘	✘	✘	✘
2013	[22]	✘	✓	✘	✘
2013	[58]	✘	✓	✘	✘
2013	[59]	✘	✓	✘	✘
2013	[60]	✘	✓	✘	✘
2013	[61]	✘	✓	✘	✘
2013	[62]	✘	✓	✘	✘
2013	[63]	✘	✓	✘	✘
2013	[64]	✘	✓	✘	✘
2013	[65]	✘	✓	✘	✘
2014	[66]	✘	✓	✘	✘
2014	[27]	✘	✓	✘	✘
2014	[67]	✘	✘	✘	✘
2014	[68]	✘	✓	✘	✘
2014	[23]	✘	✓	✘	✘
2015	[69]	✘	✓	✘	✘
2014	[70]	✘	✘	✘	✘
2015	[28]	✘	✓	✘	✘
2015	[26]	✘	✓	✘	✘
2016	[21]	✘	✓	✘	✘
2016	[71]	✓	✓	✓	✘
2016	[72]	✓	✓	✓	✘
2017	[73]	✘	✓	✘	✘
2017	[37]	✓	✓	✓	✘
2017	[74]	✓	✓	✓	✘
2018	[75]	✓	✓	✓	✘
2019	[76]	✓	✓	✓	✘
2020	[34]	✓	✓	✓	✘
2020	[33]	✓	✓	✓	✘
2021	[38]	✘	✓	✘	✘
2022	[77]	✓	✓	✓	✘
2022	[78]	✓	✓	✓	✘
2022	[79]	✘	✓	✘	✘
2023	[80]	✘	✓	✘	✘
2023	[9]	✓	✓	✓	✘

III. METHODOLOGY

In this study, the design science research [81] was deployed to develop a conceptual framework for gathering and analyzing data from suspicious database systems. Developing and evaluating artifacts, such as frameworks, models, and prototypes is a key component to design science research methodology [82]. This methodology has been found suitable for addressing complex problems and developing innovative solutions.

As Figure 1 illustrates, four distinct steps made up the followed methodology. To begin the process, the first step was to determine the search engines to be used throughout the study. Selecting the right search engine is crucial for any research as it determines the depth and breadth of the data collected. In addition to IEEE Explorer, Web of Science, Scopus, Springer Link, and Google Scholar, five more search engines were identified. The second step of the methodology was to collect data. During this process, keywords such as "Database Forensics" and "Blockchain technology" were searched. In the third step, the data acquired from the search engines were filtered based on the information gathered. This step was taken to ensure that the collected data were relevant and aligned with the objectives of the study. In addition to removing any redundant or irrelevant information that may be present in a data set, filtering makes the analysis focused.

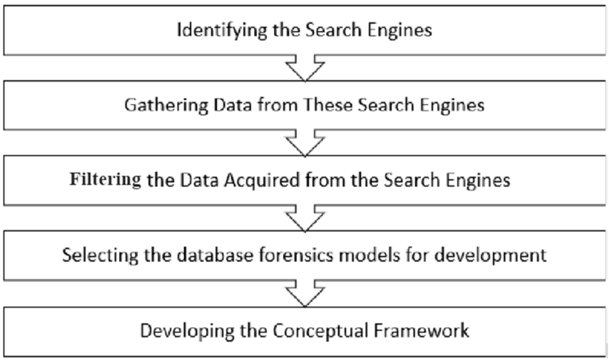
Identifying the Search Engines
Gathering Data from These Search Engines
Filtering the Data Acquired from the Search Engines
Selecting the database forensics models for development
Developing the Conceptual Framework

Fig. 1. The developed methodology.

A database forensics model was then developed, as part of the fourth step of the methodology. In this step, the appropriate models for the study were determined. As a result of the selection of models, the data gathered from the search engines were analyzed and interpreted, and then insights were generated. By developing a novel conceptual framework, a suitable process for integrating and analyzing the data in databases was outlined. By using this framework as a guide for the research process, the data could be handled and interpreted in a systematic and rigorous manner. This paper presents a clearly structured methodology, allowing the researchers to gather, filter, and analyze data in an effective way.

IV. RESULTS AND DISCUSSION

A novel conceptual framework was developed based on the findings of this study to enable the gathering and analysis of data of database systems using blockchain technology. The developed framework consists of two main stages: data gathering and data analysis (see Figure 2).

A. Data Gathering Stage

This stage is used to gather data from the database in question. It involves five processes:

- *Data Acquisition*: It is first necessary to acquire the relevant data from the database systems deploying blockchain technology. As a result, either the data can be extracted directly from the database system or forensic tools can be utilized to retrieve the data from the system once they have been extracted.
- *Data Encryption*: Encrypting the data before they are stored on blockchain ensures their integrity and confidentiality. To accomplish this, encryption algorithms can be applied at the source.
- *Data Validation*: To ensure the accuracy and reliability of the data gathered, it is essential to validate them. It may be a good idea to consider any anomalies, inconsistencies, or inaccuracies in the data when making any kind of analysis. When errors or issues are discovered during the data validation process, data analysis can be adversely affected.
- *Data Hashing*: A hashing algorithm is a cryptographic technique for condensing a large quantity of information into a short and fixed-length string. The data are made resistant to tampering by hashing, which means that they cannot be altered or corrupted in any way. Before storing the data on a blockchain, it is necessary to hash them so that their integrity and authenticity can be verified before being stored on the blockchain.
- *Data Incorporation*: Data can be incorporated into a blockchain once they have been gathered, validated, and hashed. Data integrity is ensured, and secure transmission and analysis are facilitated by the blockchain, which acts as a decentralized ledger.

B. Data Analysis Stage

In this stage, the gathered and preserved data will be analyzed to discover database incidents. This stage involves five processes:

- *Data Storage*: The data gathered during the process are stored on the blockchain and can be accessed by authorized users if they possess the proper permissions. The immutable nature of blockchain ensures that the data stored on it cannot be tampered with, which ensures that they are authentic and trustworthy.
- *Data Retrieval*: Specialized tools and techniques can be used to access and analyze blockchain data. Data can be extracted and analyzed applying blockchain analysis software or by querying the blockchain utilizing a blockchain explorer.
- *Data Visualization*: The visual presentation of data can simplify the understanding and interpretation of the analyzed information. Trends and patterns can be communicated with visual representations, such as graphs, charts, and dashboards.
- *Data Analysis Techniques*: In order to derive meaningful insights and findings from the gathered data, various methods of data analysis can be applied. There are many techniques that can be adopted to analyze data, such as statistical analysis, machine learning, and data mining. With the deployment of these techniques, forensic investigators can gain a deeper understanding of the data and identify possible evidence or leads that could aid the latter's investigation.

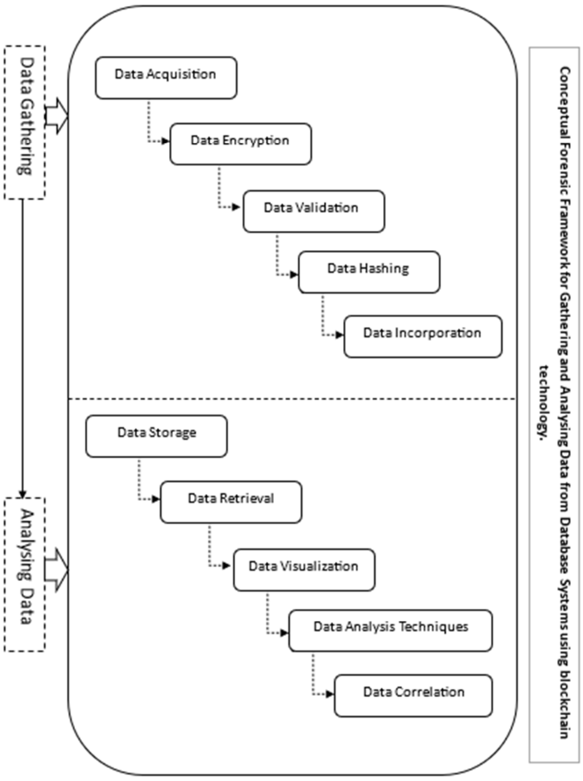

Fig. 2. The conceptual framework for gathering and analyzing data from database systems using blockchain technology.

- *Data Correlation*: Correlation analysis can be performed to find the relationships between different data that have been collected. It is possible for forensic investigators to uncover hidden patterns or connections that may have previously been hidden by analyzing the correlations between different data sources using the correlation analysis.

C. Discussion

This section discusses the findings of this study from two dimensions: benefits and comparison. The first dimension explores the benefits of the developed conceptual framework for gathering and analyzing data of database systems using blockchain technology. The second dimension compares the developed framework with the existing database forensics models. Figure 3 displays the two dimensions covered in this section. The first dimension discussed the developed framework from four perspectives:

- *Security:* Blockchain-based databases have a significant advantage in terms of security when compared to traditional database systems. One of the most important features of blockchain technology is its decentralized architecture. The data are stored in multiple nodes rather than in a central database. The decentralized approach makes data access more difficult for hackers since they would need to penetrate multiple nodes simultaneously to gain access to and manipulate the data. In addition, blockchain technology provides greater integrity to data in a more secure manner. Every transaction on the blockchain is validated and verified by the network of nodes, which means that data can never be altered in any way by anyone. Furthermore, the built-in verification process not only ensures the data are accurate and verifiable, but also improves the security of the database.

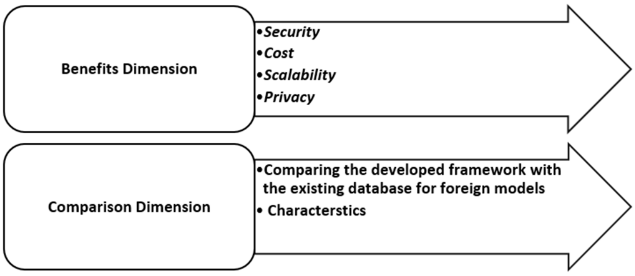

Fig. 3. The dimensions considered in this study.

- *Cost:* Blockchain technology has certain potential disadvantages, but it offers several benefits, and it is important to consider them before adopting it. The drawback of blockchain-based database systems is that they are very expensive in comparison to other systems. In order for an organization to take advantage of the potential benefits of blockchain technology, it must significantly invest in infrastructure and expertise, especially if this organization is relatively new to the technology. As a result, it is important to maintain and upgrade blockchain systems continually. However, in the long run, blockchain technology can generate cost savings and contribute to long-term sustainability. By eliminating intermediaries and diminishing the need for trust, blockchain reduces operational costs. Additionally, the decentralized architecture of blockchain allows for more efficient management of data, which ultimately results in cost savings.
- *Scalability*: The blockchain technology is also a very good option when it comes to database systems since it is capable of handling large volumes of data successfully. Thanks to its distributed architecture, the blockchain system can competently scale. This system can be expanded to accommodate more nodes as the database grows, which allows the database capacity to be increased as needed due to the addition of supplementary users to the network. The scalability of the system means that it is particularly beneficial for industries that produce large quantities of transactional data, such as those in the field of financial services and those in the supply chain sector. Consequently, it should be noted that blockchain scaling has some limitations that need to be considered before using it. Additionally, as the size of the network grows, the computing power and storage capacity that are required to validate the transactions in that network will also grow proportionally with the increase in its size. This can affect both cost and performance of the system. Moreover, the consensus mechanisms of blockchain may not be the most effective way to process complex queries or to gain access to real-time data in the future as they are not the most efficient methods for tackling complex problems.
- *Privacy:* Several studies have demonstrated the benefits of blockchain technology for data management systems, including enhanced privacy. The decentralized nature of blockchain technology prevents hackers or third parties from accessing sensitive information because the data are stored on multiple nodes across the network. Blockchain data can only be viewed or updated by parties who are authorized to view or update them due to the embedded consensus mechanism. It is important to consider the possibility of privacy threats posed by blockchain technology despite the benefits it has for many businesses. Data could accidentally or intentionally leak from the blockchain. Furthermore, blockchain's anonymity may not be suited to applications that require identity verification. If the privacy of individuals and entities is not adequately protected, blockchain's transparency could compromise it.

The second dimension is the comparison of the developed framework with those proposed in existing studies. The developed framework leverages blockchain technology to gather and analyze data of database systems. As can be seen in Table II, there are no existing traditional database forensic investigation models that incorporate blockchain technology. The known database forensic investigation models gather and analyze data using traditional methods and tools. Blockchain technology can contribute to the investigation process in many ways and these models often overlook its potential assets. A blockchain-based conceptual framework provides a more comprehensive and efficient approach to database forensic investigations. Blockchain technology can be utilized to create immutable audit trails in this context. A distributed ledger is created by blockchain technology, ensuring that every transaction and change can be verified and recorded. As a result, data collected during an investigation are more transparent and reliable, providing a more robust basis for analysis. Further, blockchain technology simplifies the forensic investigation process by introducing the concept of smart contracts. Unlike traditional contracts, smart ones are self-executing contracts in which the terms of the purchase agreement are directly written into code. Forensic investigations of databases often engage smart contracts to define rules and procedures for collecting and analyzing data. Therefore, investigations can be streamlined, and data gathering and analysis can be consistently and accurately performed.

In addition, the developed conceptual framework makes use of blockchain technology to enhance data security and confidentiality. It is possible to securely store and access sensitive data with the cryptographic mechanisms of blockchain without compromising their integrity. When investigating sensitive data in database forensics, this is especially important.

TABLE II. COMPARISON OF THE DEVELOPED DATABASE FORENSICS FRAMEWORK WITH THE EXISTING MODELS

Year	Existing models	Gathering and protecting stage	Rebuilding and analyzing stage	Documenting and presenting stage	Blockchain technology
2004	[83]	✘	✘	✘	✘
2004	[24]	✘	✘	✘	✘
2004	[84]	✓	✓	✓	✘
2007	[39]	✘	✘	✘	✘
2007	[40]	✘	✘	✘	✘
2007	[41]	✘	✘	✘	✘
2007	[42]	✘	✓	✘	✘
2007	[43]	✘	✓	✘	✘
2007	[44]	✘	✓	✘	✘
2007	[45]	✘	✓	✘	✘
2007	[46]	✘	✓	✘	✘
2008	[20]	✓	✓	✓	✘
2008	[47]	✘	✓	✘	✘
2006	[48]	✘	✓	✘	✘
2009	[14]	✘	✓	✘	✘
2009	[12]	✘	✓	✘	✘
2010	[49]	✘	✓	✘	✘
2011	[50]	✘	✘	✘	✘
2011	[51]	✘	✘	✘	✘
2011	[15]	✘	✘	✘	✘
2011	[52]	✘	✘	✘	✘
2012	[16]	✘	✓	✘	✘
2012	[17]	✓	✓	✓	✘
2012	[18]	✓	✓	✓	✘
2012	[53]	✘	✘	✘	✘
2012	[54]	✘	✓	✘	✘
2012	[55]	✘	✓	✘	✘
2012	[56]	✘	✓	✘	✘
2012	[57]	✘	✘	✘	✘
2013	[22]	✘	✓	✘	✘
2013	[58]	✘	✓	✘	✘
2013	[59]	✘	✓	✘	✘
2013	[60]	✘	✓	✘	✘
2013	[61]	✘	✓	✘	✘
2013	[62]	✘	✓	✘	✘
2013	[63]	✘	✓	✘	✘
2013	[64]	✘	✓	✘	✘
2013	[65]	✘	✓	✘	✘
2014	[66]	✘	✓	✘	✘
2014	[27]	✘	✓	✘	✘
2014	[67]	✘	✘	✘	✘
2014	[68]	✘	✓	✘	✘
2014	[23]	✘	✓	✘	✘
2015	[69]	✘	✓	✘	✘
2014	[70]	✘	✘	✘	✘
2015	[28]	✘	✓	✘	✘
2015	[26]	✘	✓	✘	✘
2016	[21]	✘	✓	✘	✘
2016	[71]	✓	✓	✓	✘
2016	[72]	✓	✓	✓	✘
2017	[73]	✘	✓	✘	✘
2017	[37]	✓	✓	✓	✘
2017	[74]	✓	✓	✓	✘
2018	[75]	✓	✓	✓	✘
2019	[76]	✓	✓	✓	✘
2020	[34]	✓	✓	✓	✘
2020	[33]	✓	✓	✓	✘
2021	[38]	✘	✓	✘	✘
2022	[77]	✓	✓	✓	✘
2022	[78]	✓	✓	✓	✘
2022	[79]	✘	✓	✘	✘
2023	[80]	✘	✓	✘	✘
2023	[9]	✓	✓	✓	✘
2023	Proposed	✓	✓	✓	✓

V. CONCLUSION

A blockchain can be viewed as a distributed database that supports the sharing of records of transactions among its members. To prevent a fraudulent transaction from taking place, the majority of the members must confirm each and every transaction. It has been generally established that once a record is created and accepted by the blockchain, it cannot be altered or deleted by anyone. Several studies conducted in the digital forensics field have proposed that blockchain technology can be integrated as a part of their digital forensics work. Consequently, it is rare to find such technology being used in database forensic investigations. This paper contributes to the relevant body of knowledge by purposing a novel conceptual framework for forensic analysis of data collected from database systems by implementing blockchain technology that provides a novel method for collecting and analyzing such data. It is the first time that blockchain technology is used in database forensics in order to trace digital evidence.

The design science research method was adopted to accomplish the objectives of the research. The findings of this study revealed that with the developed framework for forensic analysis, it would be possible to gather and analyze database incidents in a more efficient manner than with the employment of the existing models. In future research, the database forensics framework developed in the present paper can be implemented in real scenarios to evaluate its effectiveness and practicality.

ACKNOWLEDGMENT

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-23-DR-83). Therefore, the authors thank the University of Jeddah for its technical and financial support

REFERENCES

[1] A. Al-Dhaqm, S. Abd Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," *Jurnal Teknologi*, vol. 78, no. 6–11, pp. 45–57, Jun. 2016, https://doi.org/10.11113/jt.v78.9190.

[2] S. Olnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, Sep. 2017, https://doi.org/10.1016/j.giq.2017.09.007.

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

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

[5] S. K. Singh and A. Mishra, "Digital Forensics and Cybersecurity Tools," in *Advancements in Cybercrime Investigation and Digital Forensics*, 1st Edition., Cambridge, MA, USA: Academic Press, 2023, pp. 367–382.

[6] V. Jyotinagar and B. Meshram, "Digital forensic analysis of attack detection and identification in private cloud environments for databases," *Journal of Integrated Science and Technology*, vol. 12, no. 4, pp. 798–798, Jan. 2024, https://doi.org/10.62110/sciencein.jist.2024.v12.798.

[7] A. M. R. Al-Dhaqm, "Simplified Database Forensic Invetigation Using Metamodeling Approach," Ph.D. dissertation, University of Technology Malaysia, Johor, Malaysia, 2019.

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

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

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

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

[12] D. Lee, J. Choi, and S. Lee, "Database Forensic Investigation Based on Table Relationship Analysis Techniques," in *2nd International Conference on Computer Science and its Applications*, Jeju, Korea (South), Dec. 2009, pp. 1–5, https://doi.org/10.1109/CSA.2009.5404235.

[13] J. Choi, K. Choi, and S. Lee, "Evidence Investigation Methodologies for Detecting Financial Fraud Based on Forensic Accounting," in *2nd International Conference on Computer Science and its Applications*, Jeju, Korea (South), Dec. 2009, pp. 1–6, https://doi.org/10.1109/CSA.2009.5404202.

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

[15] 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*, Loutraki, Greece, Jun. 2011, pp. 164–171, https://doi.org/10.1007/978-3-642-22339-6_20.

[16] S. Tripathi and B. B. Meshram, "Digital Evidence for Database Tamper Detection," *Journal of Information Security*, vol. 3, pp. 113–121, Apr. 2012, https://doi.org/10.4236/jis.2012.32014.

[17] H. K. Khanuja and D. S. Adane, "A Framework for Database Forensic Analysis," *Computer Science & Engineering: An International Journal*, vol. 2, no. 3, pp. 27–41, Jun. 2012, https://doi.org/10.5121/cseij.2012.2303.

[18] R. Susaimanickam, "A workflow to support forensic database analysis," Ph.D. dissertation, Murdoch University, Perth, Western Australia, 2012.

[19] A. S. Alraddadi, "A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11505–11510, Aug. 2023, https://doi.org/10.48084/etasr.6128.

[20] K. Fowler, *SQL Server Forenisc Analysis*. London, UK: Pearson Education, 2008.

[21] 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," Ph.D. dissertation, University of Nairobi, Nairobi, Kenya, 2016.

[22] H. Khanuja and D. Adane, "Forensic Analysis of Databases by Combining Multiple Evidences," *International Journal of Computers and Technology*, vol. 7, no. 3, pp. 654–663, Dec. 2008, https://doi.org/10.24297/ijct.v7i3.3446.

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

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

[25] K. Fowler, *A Real World Scenario of a SQL Server 2005 Database Forensics Investigation*. Emergis Inc., 2007.

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

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

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

[29] R. Chopade and V. K. Pachghare, "Ten years of critical review on database forensics research," *Digital Investigation*, vol. 29, pp. 180–197, Jun. 2019, https://doi.org/10.1016/j.diin.2019.04.001.

[30] C. Orosco, C. Varol, and N. Shashidhar, "Graphically Display Database Transactions to Enhance Database Forensics," in *8th International Symposium on Digital Forensics and Security*, Beirut, Lebanon, Jun. 2020, pp. 1–6, https://doi.org/10.1109/ISDFS49300.2020.9116412.

[31] B. Z. Adamu, M. Karabatak, and F. Ertam, "A Conceptual Framework for Database Anti-forensics Impact Mitigation," in *8th International Symposium on Digital Forensics and Security*, Beirut, Lebanon, Jun. 2020, pp. 1–6, https://doi.org/10.1109/ISDFS49300.2020.9116375.

[32] R. Marsh, S. Belguith, and T. Dargahi, "IoT Database Forensics: An Investigation on HarperDB Security," in *3rd International Conference on Future Networks and Distributed Systems*, Paris, France, Jul. 2019, pp. 1–7, https://doi.org/10.1145/3341325.3341993.

[33] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response

Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, pp. 145018–145032, 2020, https://doi.org/10.1109/ACCESS.2020.3008696.

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

[35] R. Chopade and V. Pachghare, "Data Tamper Detection from NoSQL Database in Forensic Environment," *Journal of Cyber Security and Mobility*, vol. 10, no. 2, pp. 421–450, Apr. 2021, https://doi.org/10.13052/jcsm2245-1439.1025.

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

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

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

[39] M. J. Malmgren, "An infrastructure for database tamper detection and forensic analysis," Ph.D. dissertation, University of Arizona, Tucson, AZ, USA, 2007.

[40] D. Litchfield, *Oracle Forensics Part 4: Live Response*. Next Generation Security Software Ltd, 2007.

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

[42] D. Litchfield, *Oracle Forensics Part 1: Dissecting the Redo Logs*. Next Generation Security Software Ltd, 2007.

[43] D. Litchfield, *Oracle Forensics Part 2: Locating Dropped Objects*. Next Generation Security Software Ltd, 2007.

[44] D. Litchfield, *Oracle Forensics Part 5: Finding Evidence of Data Theft in the Absence of Auditing*. Next Generation Security Software Ltd, 2007.

[45] D. Litchfield, *Oracle Forensics Part 6: Examining Undo Segments, Flashback and the Oracle Recycle Bin*. Next Generation Security Software Ltd, 2007.

[46] D. Litchfield, *Oracle Forensics Part 7: Using the Oracle System Change Number in Forensic Investigations*. Next Generation Security Software Ltd, 2007.

[47] K. E. Pavlou and R. T. Snodgrass, "Forensic analysis of database tampering," *ACM Transactions on Database Systems*, vol. 33, no. 4, Sep. 2008, Art. no. 30, https://doi.org/10.1145/1412331.1412342.

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

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

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

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

[52] H. Beyers, M. Olivier, and G. Hancke, "An approach to examine the Metadata and Data of a database Management System by making use of a forensic comparison tool," ISSA, Jan. 2011.

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

[54] P. D. Abhonkar and A. Kanthe, "Enriching Forensic Analysis process for Tampered Data in Database," *International Journal of Computer Science and Information Technologies*, vol. 3, no. 5, pp. 5078–5085, 2012.

[55] K. E. Pavlou and R. T. Snodgrass, "DRAGOON: An Information Accountability System for High-Performance Databases," in *28th International Conference on Data Engineering*, Arlington, VA, USA, Apr. 2012, pp. 1329–1332, https://doi.org/10.1109/ICDE.2012.139.

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

[57] H. Q. Beyers, M. S. Olivier, and G. P. Hancke, "Arguments and Methods for Database Data Model Forensics," in *Seventh International Workshop on Digital Forensics & Incident Analysis*, Crete, Greece, Jun. 2012, pp. 139–149.

[58] K. E. Pavlou and R. T. Snodgrass, "Generalizing database forensics," *ACM Transactions on Database Systems*, vol. 38, no. 2, Apr. 2013, Art. no. 12, https://doi.org/10.1145/2487259.2487264.

[59] O. M. Adedayo and M. S. Olivier, "On the Completeness of Reconstructed Data for Database Forensics," in *4th International Conference on Digital Forensics and Cyber Crime*, Lafayette, LA, USA, Oct. 2012, pp. 220–238, https://doi.org/10.1007/978-3-642-39891-9_14.

[60] P. P. Gawali and S. R. Gupta, "Forensic Analysis Algorithm: By using the Tiled Bitmap with Audit Log Mechanism," *International Journal of Computer Applications*, vol. 63, no. 11, pp. 36–42, Feb. 2013, https://doi.org/10.5120/10513-5483.

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

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

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

[64] P. P. Gawali, "Database Tampering and Detection of Data Fraud by Using the Forensic Scrutiny Technique," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 2, pp. 439–446, 2013.

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

[66] M. Xu *et al.*, "A Reconstructing Android User Behavior Approach based on YAFFS2 and SQLite," *Journal of Computers*, vol. 9, no. 10, pp. 2294–2302, Oct. 2014, https://doi.org/10.4304/jcp.9.10.2294-2302.

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

[68] H. Q. Beyers, "Database forensics: Investigating compromised database management systems," M.S. thesis, University of Pretoria, Pretoria, South Africa, 2013.

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

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

[71] A. Aldhaqm, S. A. Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge," *Research Journal of Applied*

Sciences, Engineering and Technology, vol. 12, no. 4, pp. 386–394, Feb. 2016, https://doi.org/10.19026/rjaset.12.2377.

[72] A. Al-dhaqm, S. Razak, S. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," *Jurnal Teknologi*, vol. 78, pp. 45–57, Jun. 2016, https://doi.org/10.11113/jt.v78.9190.

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

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

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

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

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

[78] N.-A. Le-Khac and K.-K. R. Choo, *A Practical Hands-on Approach to Database Forensics*. New York, NY, USA: Springer, 2022.

[79] K. Moser, K.-K. R. Choo, and N.-A. Le-Khac, "Database Forensics for Analyzing Data Loss in Delayed Extraction Cases," in *A Practical Hands-on Approach to Database Forensics*, N.-A. Le-Khac and K.-K. R. Choo, Eds. New York, NY, USA: Springer, 2022, pp. 175–232.

[80] M. I. Nissan, J. Wagner, and S. Aktar, "Database memory forensics: A machine learning approach to reverse-engineer query activity," *Forensic Science International: Digital Investigation*, vol. 44, Mar. 2023, Art. no. 301503, https://doi.org/10.1016/j.fsidi.2023.301503.

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

[82] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, "Research Challenges and Opportunities in Drone Forensics Models," *Electronics*, vol. 10, no. 13, Jan. 2021, Art. no. 1519, https://doi.org/10.3390/electronics10131519.

[83] R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper Detection in Audit Logs," in *30th VLDB Conference*, Toronto, ON, Canada, 2004, pp. 504–515.

[84] P. M. Wright, "Oracle Database Forensics using LogMiner," presented at the June 2004 Conference, SANS Institute, 2004.