Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Structuring and organizing database security domain from big data perspective using meta-modeling approach

Ahmad Alshammari *

Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha, Saudi Arabia

ARTICLE INFO

Article history:
Received 27 September 2023
Received in revised form
16 January 2024
Accepted 31 January 2024

Keywords:
Database security
Meta-modeling
Data protection
Access control
Big data security

ABSTRACT

Database security is an area focused on safeguarding databases against harmful access. It involves ensuring data accuracy, blocking unauthorized entry, and preventing harmful code within the database. Although various security models and methods exist, they often don't comprehensively cover all aspects of database security. This leads to a diverse and unclear understanding of database security among experts. This study proposes a unified framework, the Database Security Meta-model (DBSM), which acts as a standard language in this field. The DBSM, comprising twelve main elements, is thoroughly vetted to align with security needs and offers guidelines for practitioners to create specific security solutions.

1. Introduction

Information systems and other functions that make up the operational processes in most organizations today have been automated, whether they are administrative, educational, governmental, or social. Thus, the security of databases is of the utmost importance to these organizations. To proceed further, it is essential that we first discuss what database security means. The database security field is a part of the cybersecurity domain when it comes to protecting the confidentiality, integrity, and availability of sensitive information stored within the database (Lessambo, 2023). This is a very significant aspect of the organization's security posture. It ensures the protection of sensitive data using specialized security controls, such as authentication, encryption, logging, and access control (Tall and Zou, 2023). In the literature, a wide range of database security models, frameworks, techniques, and mechanisms have been proposed. However, these models, frameworks, and methodologies were proposed from a practical perspective (Alhussan et al., 2022a; Alshammari, 2023a). Although some organizations have developed their security frameworks and guidelines based on standards from the National Institute of Standards and Technology (NIST) and ISO27001, there is still no suitable model or framework for organizing, structuring, and managing database security from a conceptual viewpoint. Meanwhile, big data has emerged as a crucial topic in both industry and academia over the past few years (Alhazmi et al., 2022). There are two sides to big data, and those sides can be both positive and negative in nature (Ratner, 2003). People can take advantage of its convenience, but it is also associated with some risks as well. The collection, storage, and analysis of data have the potential to easily result in the leakage of sensitive personal information and make it difficult to comprehend the information as it is being collected, compiled, and used (George et al., 2016; Yafooz et al., 2020). There is a wide range of discussion in the current study stage regarding the importance of securing the security and privacy of large data sets. As a result of the numerous security threats that big data is frequently exposed to, this is something that must be taken seriously. Although many of these threats are common in small businesses, vulnerability is an important factor in large corporations because they hold sensitive data that is used by more than one department and several people at once. Attacks can be carried out by three types of people, namely, intruders, insiders, and administrators. It can be said that an intruder is an unauthorized user who repeatedly manipulates a computer to get useful information from it. There is one type of dependable user who violates permission and tries to access information outside of the boundaries of his or her own allocation, and that user is known as an insider. An administrator is a

* Corresponding Author.
Email Address: ahmad.Almkhaidsh@nbu.edu.sa
https://doi.org/10.21833/ijaas.2024.02.019
Corresponding author's ORCID profile:
https://orcid.org/0009-0000-2051-2757

user who has the authority to control a computer system but abuses that authority by spying on the activity of a database management system (DBMS) and acquiring sensitive data, which is contrary to the organization's security regulations related to data security (Kulkarni and Urolagin, 2012; Teimoor, 2021).

The importance of using data for decision-making in organizations has grown significantly, along with the increase in cyber threats in both number and severity. As a result, securing databases has become a crucial task for these organizations. From this perspective, the proposed database security meta-model (DBSM) is vital for efficiently organizing and managing database security. This meta-model offers significant advantages, including a comprehensive view of security management within a database environment and a structured framework for organizing security measures.

The proposed meta-model integrates various components of information security by defining their relationships and interactions. It also aids in identifying, categorizing, and organizing information and security elements within a database, thereby enhancing efficiency in data management. Consequently, this meta-model is beneficial for both database administrators and security professionals. It promotes standardized security management, improves collaboration, and enhances knowledge sharing within organizations. Enhanced security operations lead to quicker incident responses and reduced potential breaches. Therefore, DBSMs are essential for robust database security, simplifying administration, enhancing security, and supporting regulatory compliance.

As a result, the data security area is organized and structured using a meta-modeling approach. A meta-modeling technique involves developing models based on the models that have been built (Wąsowski and Berger, 2023). The DBSM was developed because of this research. A DBSM provides a comprehensive and organized approach to database security. Database security mechanisms can be defined, analyzed, and evaluated using this tool. It is also able to integrate numerous security components into a single, integrated security system with DBSM. The DBSM enables the integration of various security components into a cohesive and comprehensive security strategy. This meta-model improves security within a database environment by combining and harmonizing different security measures. Traditionally, organizations have deployed multiple security solutions to protect their databases, often resulting in decentralized control and disjointed security mechanisms. This fragmented approach can compromise data confidentiality, integrity, and availability, leading to security inefficiencies and gaps.

The DBSM addresses these challenges by integrating diverse security components into a structured and unified framework. This integration allows organizations to manage access control, user authentication, data encryption, and auditing more effectively. As a result, a stronger and more efficient defense against potential threats is established through improved coordination, collaboration, and management.

One of the key benefits of this meta-model is its ability to streamline security operations. By centralizing security components, the DBSM enhances visibility and control over an organization's database infrastructure. This centralization reduces the risks of misconfigurations and unauthorized access by enabling more effective management and administration of security policies, user privileges, and audit logs.

Additionally, the DBSM promotes interoperability and standardization across the industry. Developers and security vendors can utilize this common framework to design and implement security solutions more effectively. This interoperability ensures that various security management tools and technologies within a company can be fully utilized without compromising compatibility or the overall security posture of the organization.

By utilizing a DBSM, it is possible to achieve an efficient and comprehensive approach to database security. Using integrated security systems is an effective way to enhance the overall security posture of the organization, streamline security operations, and enhance interoperability between different security technologies to improve security posture. This meta-model can be implemented to significantly increase the protection of sensitive data and minimize the risks associated with unauthorized access and database breaches by implementing this key design principle.

The paper is organized as follows: The related works are discussed in Section 2, and the methodology is discussed in Section 3. Section 4 presents the results and discussion, while Section 5 introduces the research questions and answers. Finally, Section 6 provides the conclusions and future directions of the study.

2. Related works

A considerable amount of attention has been paid to database security since the mid-1970s, ranging from discretionary security for System R and Ingres to access control models and multilevel database systems, as well as security for emerging data management systems, data privacy, privacy-preserving data mining, data mining for security applications, and privacy and security associated with big data. Several researchers have paid more attention to the big data security area in various domains. For example, Albalawi (2018) proposed an innovative framework and idea in order to achieve better security online for sensitive pieces of information. This framework carries out the task of protecting private information by giving the last decision to the selected admin regarding who can view such info and who can't. In addition, this framework also focuses on what is considered private or sensitive data to give the option to the

admin who can view the data. Khan et al. (2018) studied the structures of SQL queries to model behaviors and identify suspicious access to RDBMS using techniques such as mining frequent and rare item sets. Additionally, their research highlighted the significance of where and how databases are stored and discussed methods to enhance the protection of these databases from unauthorized access.

According to Odirichukwu and Asagba's (2017) projected work, the authors acknowledge that with the rapid growth of the internet every day and the rapid growth of businesses, many businesses post their data online for others to view and see. The data that is uploaded online can, however, be manipulated by unauthorized users on the web, so this paper raises awareness about such matters so businesses can be more cautious when uploading data to the public eye. Odirichukwu and Asagba (2017) presented the idea of how many modern applications need a better level of security that saves data from internal breaches in the blockchain by using cloud databases. It also notes that cloud databases should include a reliable authority figure to ensure a higher level of security efficiency. It acknowledges that the proposed cloud database system could potentially be manipulated or altered by unauthorized personnel to meet individual needs. Gruschka et al. (2018) reviewed the current state of legal guidelines and examined various data protection and privacy preservation techniques for big data analysis, as well as the pieces of information that may be at risk of compromising the privacy of individuals. It is mentioned several times in the proposed work that the privacy techniques employed are compliant with the legal requirements and that two case studies were used to examine how privacy-preserving techniques might be implemented. According to Zhang (2018), data protection and privacy are considered to be vital issues in today's world. Besides, the law exists where it protects individuals' privacy online. However, people still need to be held accountable and pay attention to their own privacy online. They need to take all measures and needs necessary to protect sensitive data from being leaked by data breaches. Additionally, Al-Dwairi et al. (2018) discussed the vulnerability of cloud computing to impersonation attacks. As a solution, they proposed a method to detect masquerade attacks in cloud environments. This method involves detecting sequences of correlated system calls from VMs and analyzing NetFlow data from the network environment. Similarly, Adedayo and Olivier (2014) highlighted how the security of Big Data can be improved by using the Blockchain as an extra layer of security. This security solution is empowered by blockchain technology and incorporates fragmentation, encryption, and access control techniques. The fact that the issue of big data security has not been discussed before has been mentioned in the proposed work. Awadallah et al. (2021) addressed the issue of how prone cloud services are to attacks, and a scheme was made to combine blockchain and cloud technology to solve this issue. A tamper-free cloud computing environment was achieved through this scheme. In addition, Yaseen et al. (2017) presented a way to overcome the issue of PEP-side caching, which can be exploited by insiders to bypass cloud access control mechanisms. This was achieved by creating a manageable model that detects and prevents insider threats on the PEP side. Also, Chaudhary et al. (2021) pointed out the weak spots of security for Big Data and IoT. XSS attack is one such security attack that helps the attacker to enter the user's private data. Preventing XSS attacks was the main topic for the projected paper. Datasets that were used for building the most accurate CNN model were tested for the detection of XSS attacks. Finally, Liu et al. (2020) focused on the economic perspective of Big Data attacks and how these data breaches affect the financial status of the victim. Whether it's from blackmail or fraud, some even go as far as theft of intellectual property. The objective was to provide economic justification for technical decisions taken to protect big data and the costs that organizations often spend on it.

In addition, a few digital forensics works have been proposed as a method of detecting and investigating the threats and risks facing organizations. The use of digital forensics can be a very powerful tool in helping organizations identify potential security threats and incidents, mitigate risks, and improve their overall security posture by utilizing digital forensics to reduce risks. Numerous works have been suggested and created by the authors (Ngadi et al., 2012; Al-Dhaqm et al., 2021; 2020a; 2020b; 2020c; 2023a; 2023b; Ali et al., 2018; 2015; Kebande and Ray, 2016; Kebande and Venter, 2016; Kebande et al., 2020; Saleh et al., 2021; 2023; Alhussan et al., 2022b; Alshammari, 2023b; Salem et al., 2023; Ullah et al., 2023) to examine and identify cybercrime, data cracks, and other digital risks to organizations. Table 1 displays the advantages and disadvantages of the existing database security work. As shown in Fig. 1, database security can be characterized as heterogeneous and ambiguous by the advantages and disadvantages shown in Table 1. Since database security encompasses a wide range of challenges and complexities, it requires a structured and organized approach. DBSM is developed in this study to meet this need. In meta-models, a domain's essential components and relationships are represented and understood at high levels. The use of meta-models can facilitate the conceptualization, analysis, and design of effective security measures. By implementing database security management, you can ensure the security of your databases in an organized and comprehensive manner. An auditing procedure is followed, along with strategies for managing risk, as well as mechanisms for access control, encryption algorithms, and authentication protocols. To accommodate evolving security threats and technologies, the meta-model must be adaptable and scalable. Using the meta-model effectively requires a learning curve.

Table 1: Advantages and disadvantages of the existing database security models

Reference	Advantages	Disadvantages
(Albalawi, 2018)	A key advantage of this framework is that it provides privacy and control. Administrators can decide who can access private information under the proposed framework. Implementing this framework allows administrators to control which users or groups are authorized to view sensitive information. As a result, private information is protected from unauthorized access. Furthermore, the framework defines what constitutes private or sensitive data. Information that should be considered private can be customized and set according to specific parameters. As a result, privacy and security are tailored to the unique needs of each online platform	1. Complexity and learning curve 2. Cost implications 3. Compatibility and integration 4. False sense of security 5. Potential for increased complexity in attack vectors
(Khan et al., 2018)	The structures of SQL queries must be considered when modeling behaviors to identify and become wary of malicious RDBMS accesses using frequent and rare item-set mining. As a result, multiple benefits can be obtained, including the ability to recognize suspicious patterns, understand the intentions behind access requests, develop baseline behavior profiles, and improve the accuracy of behavior identification models Organizations can enhance their security measures based on these advantages and protect their RDBMS from potential threats by taking advantage of these advantages	In spite of the advantages of modeling behaviors using SQL queries as a means of identifying and wary of malicious accesses to RDBMSs, it is important not to ignore the disadvantages of the structures used in these queries. Query structures with complex syntaxes, large performance overhead, and limitations in scalability should be carefully considered when developing dynamic queries. There is also limited flexibility for dynamic queries. It is important for database administrators and security professionals to understand these disadvantages in order to make informed decisions regarding the trade-offs and choose appropriate strategies to mitigate the risks associated with malicious RDBMS accesses
(Odirichukwu and Asagba, 2017)	Applications can be significantly enhanced in terms of security by implementing blockchain and cloud databases. As opposed to blockchain, cloud databases provide scalability, flexibility, robust backup, disaster recovery, and advanced security features. Blockchain offers immutability, data integrity, transparency, and accountability. With these technologies, organizations can enhance application security and protect sensitive data from cyberattacks. Choosing the most appropriate implementation strategy for blockchain and cloud databases is crucial for organizations to maximize their benefit from enhanced application security	While the idea of integrating blockchain technology with cloud databases to enhance application security holds promise, it is important to be aware of the potential disadvantages. The complexity and learning curve, scalability challenges, energy consumption, regulatory and compliance concerns, and dependence on third-party providers are crucial factors to consider. Organizations should carefully evaluate these drawbacks before deciding to implement such a system, ensuring that the benefits outweigh the associated challenges
(Gruschka et al., 2018)	Analyzed various data protection and privacy preservation techniques for big data analysis, as well as individual items of information that could compromise privacy. The proposed work mentions several times that the privacy techniques employed comply with legal requirements and that privacy-preserving techniques were examined in two case studies	It is important to acknowledge the limitations and potential disadvantages of data protection and privacy preservation techniques for big data analysis. An inadequate level of anonymization, a limited encryption scope, vulnerabilities in access control mechanisms, data loss, and increased complexity are drawbacks to consider. Nevertheless, considering privacy-preserving techniques in case studies and complying with legal requirements can contribute to more robust and effective approaches for safeguarding data privacy in big data analysis
(Zhang, 2018)	A proposed model provides data protection and privacy, both of which are regarded as vital matters nowadays. In addition, there is a law that protects individuals' online privacy. It is still necessary, however, for people to pay attention to their own privacy online and hold themselves accountable. Data breaches should be prevented by taking all necessary measures and requirements	Relying solely on a legal framework may not provide comprehensive protection, and placing the burden on individuals may leave some vulnerable
(Al-Dwairi et al., 2018)	In spite of the numerous advantages offered by cloud computing, this technology also presents a number of security risks. Impersonation attacks, which pose a significant risk to cloud systems, are detected and prevented by advanced authentication mechanisms and behavioral analytics. Furthermore, businesses and individuals can protect their data by prioritizing security measures when using cloud computing	Although cloud computing offers several benefits, it is not without drawbacks, despite its many advantages. To ensure that their data is protected from impersonation attacks, it is imperative that organizations consider the security of their data, service disruptions, and the threat of data breaches when adopting cloud-based services. As a result of the risks associated with the use of cloud computing technologies, sufficient security measures must be taken to mitigate those risks, such as choosing strong authentication protocols, encrypting data, and monitoring it on a regular basis
(Adedayo and Olivier, 2014)	The advantages of security for Big Data can be significantly improved by incorporating Blockchain as an extra layer of security. The immutability, decentralization, transparency, and auditability provided by Blockchain technology address many of the security concerns associated with Big Data. By leveraging the unique features of Blockchain, organizations can enhance the integrity, confidentiality, and availability of their Big Data, ultimately protecting it from unauthorized access and ensuring its trustworthiness	Despite the limitations of traditional security measures, it is important to note that incorporating Blockchain technology as an extra layer of security can significantly enhance the security of Big Data systems. Several disadvantages of traditional security measures are addressed by the decentralized nature, transparency, and immutability of Blockchain, making it a promising solution to enhance the security of Big Data by addressing some of those disadvantages
(Awadallah et al., 2021)	The advantages of combining blockchain and cloud technology to address vulnerabilities in cloud services are evident. Enhanced security, improved data integrity, increased transparency, enhanced scalability, and greater resilience are among the key benefits. By leveraging blockchain's decentralized and tamper-resistant nature, cloud services can be made more secure, reliable, and efficient. As businesses continue to rely on cloud services, the integration of blockchain technology becomes increasingly important to mitigate vulnerabilities and ensure the smooth operation of critical systems	Among the many factors that should be carefully weighed before adopting this approach there is the complexity of the implementation, the scalability challenges, the increased latency, the higher costs, and the regulatory challenges associated with it
(Liu et al., 2020)	Several advantages have been identified in the proposed model of looking at Big Data attacks from an economic perspective, such as improved cost-effectiveness, better risk management, and improved compliance, among others	Nevertheless, the process also presents a lot of challenges in terms of complexity and time consumption. There are several factors that contribute to financial losses for victims of such attacks, including financial losses, litigation costs, reputational damage, and the costs associated with the recovery of financial losses from these attacks. There are many advantages and disadvantages to this model, as well as financial implications to consider when adopting it to protect an organization against Big Data attacks

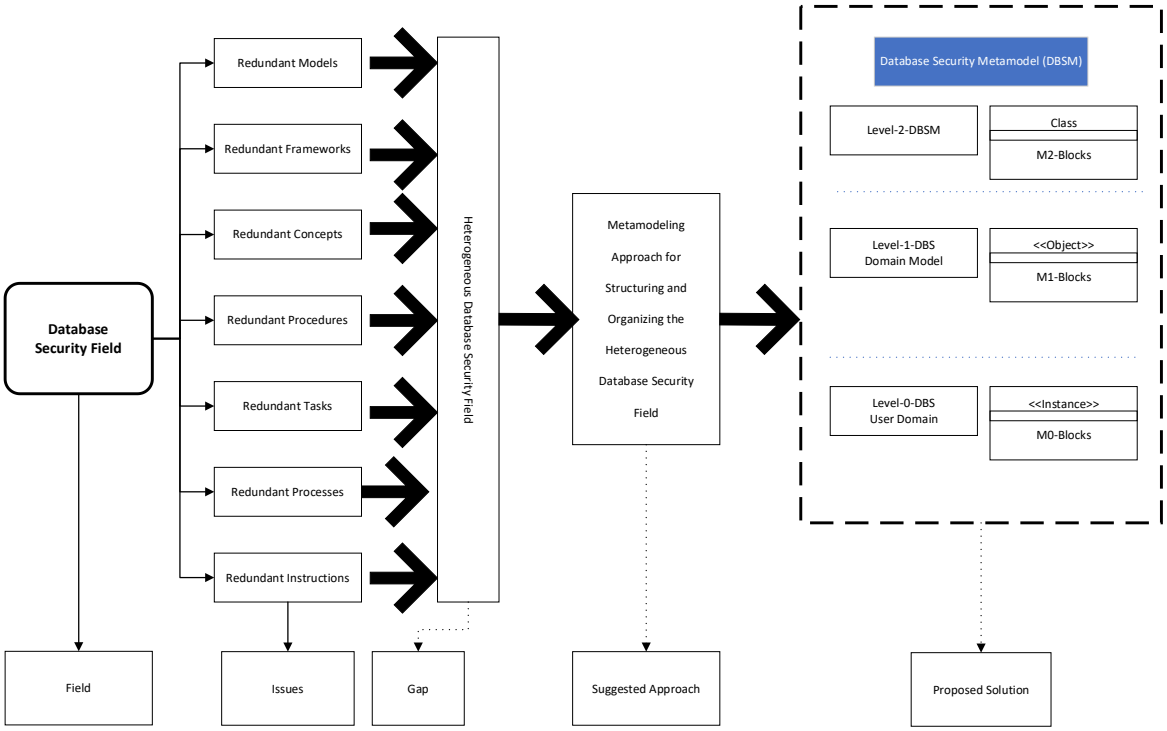

Fig. 1: Database security field issues and proposed solution

3. Methodology

A meta-modeling method is used in this work to organize and structure the database security domain. As part of the meta-modeling strategy, models of models are developed to enable analysis to find patterns and make predictions (Al-Dhaqm et al., 2020a). It is a sort of abstraction in which the model is more concerned with the design of the model than with its content. Based on the meta-modeling approach taken in this study, a model of the DBS domain is divided into components and subcomponents so that it can be studied in depth. This meta-model depicts the relationship between components and subcomponents, as well as how they interact with one another. It also includes modeling rules and instantiation stages to help you understand how the DBSM operates. Domain practitioners can simply and efficiently derive or instantiate their solution models using modeling rules and instantiation methods. The following questions are used to guide us in the development of the DBSM.

1. What are the current database security models?
2. What are the advantages and disadvantages of the current database security models?
3. Is there a meta-model for the database security domain? If yes, what are the advantages and disadvantages of it?

Therefore, the processes depicted in Fig. 2 are applied to develop the DBSM.

- Step 1. Selecting the database security models from the literature: This step involves finding and selecting database security models from common search engines (e.g., Scopus, IEEE Explorer, WOS, Springer, and Google Scholar) for the period 2010 to 2023. The author searched for the following keywords in common search engines: “Database Security,” “Database Security Management,” “Risk Management,” and “Big Data.” The results of the search included conference and journal articles, white papers, books, and book chapters related to database security and big data. These results included topics such as database security best practices, database security threats and vulnerabilities, database security solutions, database security audits, database security policies, and database security tools, database security models and frameworks. Table 2 displays the summary of searching in the common search engines.

Table2: Summary of searching in the common search engines

Search engine	Keywords	Total of articles
Scopus	“Database security"; "Database security management"; “Big data”	320
IEEE explorer		150
Springer		509
Web of Science		190
Google Scholar		228

- Step 2. Extracting security components from the selected database security models: In this step, the components will be extracted from the selected database security models based on inclusion and exclusion criteria:

a) Inclusion criteria:

- Components that are related to database security and big data security.

- Components that ensure data and system integrity, security policy, auditing, and risk assessment of the database and big data.
- Components that provide encryption and secure communication of database systems.

b) Exclusion criteria:

- Components that are not related to security.
- Components that are not related to the selected database security models.

Table 3 displays the extracted database security components from the selected database security models. The next step will propose the common database security components.

- Step 3. Proposing the common components for the database security domain: The purpose of this step is to propose common database security components based on their semantic meanings and activities. Accordingly, 12 database security components have been proposed, as shown in Table 4: Database encryption, Access control, Database authentication, Database authorization, Database security policy, Database leak prevention, Auditing database, Risk assessment and management, Database integrity, User group, Database security, and big data. Table 4 shows that there are twelve (12) components proposed for database security.

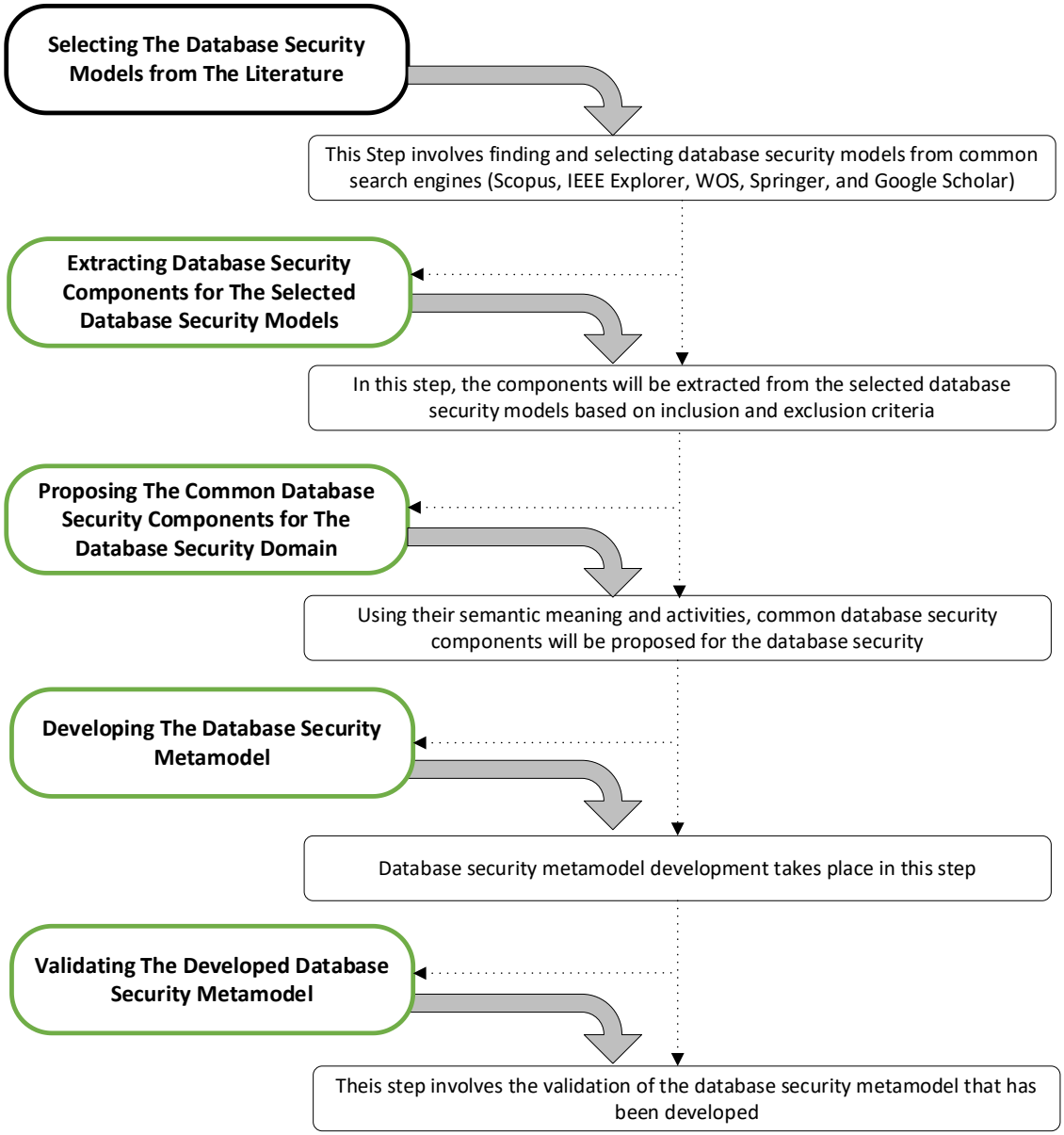

Fig. 2: Development and validation process

Table 3: Extracted database security components from the selected database security models

Access Control, Encryption, Decryption, Protection, Preservation, Firewall, Data Integrity, Repudiations, Authorization, Authentication, Data Mask, Data Threats, User Identify, Database Protection, Database Firewall, IDS, IPS, Data Encryption, Data Decryption, Auditing, Database Security Policy, Database Security Controls, Data Privacy, Data Confidentiality, Risk Assessment, Risk Control, Risk Analysis, Assess Vulnerabilities

Table 4: Proposed database security components

Proposed common database security components	Definition
Database security	A Database Security component is a component of software or hardware used to secure the confidentiality, availability, and integrity of data stored in a database. It often comprises technology for authentication, authorization, auditing, and encryption
Access control	Access control is a form of database security that governs who has access to a database and what actions those people are permitted to perform
Database authentication	Database authentication is a security mechanism used to manage database access. It entails validating a user's identification before granting them access to the database
Database authorization	An authorization process allows the database manager to get information about the user who has been authenticated. In addition to determining which database operations a user is allowed to perform, that information also determines what data objects the user can access
Database integrity	The integrity of a database is one of the most important aspects of database security. As part of this process, it is necessary to ensure that database information is accurate, consistent, and secure
Encryption database	Database encryption ensures database opacity by keeping the information hidden from unauthorized parties (e.g., intruders)
Database auditing	An audit of a database is crucial for determining if the service provider and its maintainers are complying with certain legal requirements relating to customer data protection, as well as meeting organizational standards relating to successfully protecting data assets
Big data	The big data database stores petabytes of unstructured, semi-structured, and structured data without adhering to rigid schemas. Most of these are NoSQL (non-relational) databases built on a horizontal architecture, which enables the rapid and cost-effective processing of large volumes of big data as well as multiple concurrent queries
Data leak prevention	Data leak prevention is a security approach that replaces sensitive data with a modified version of the original data
User group	A database security component that allows users to be organized into distinct groups is known as a User Group component. Administrators can simply control user access to the database by assigning privileges to each group. This prevents users from accessing sensitive data and guarantees that users only have access to the information and functions required for their job
Risk assessment and management	The process of risk management involves identifying, assessing, and prioritizing risks then taking measures to mitigate or control them. Assessing risk refers to determining the likelihood and consequences of something bad happening
Security policy	The purpose of security policies is to describe how an organization protects itself against threats, including computer security threats, and how to handle situations when they arise. A company's security policy must identify all assets and potential threats to those assets

- Step 4. Developing DBSM: This stage aims to develop the DBSM. A DBSM is a collection of security-related components and interactions that describe and analyze an enterprise's database security. As shown in Fig. 3, a schematic of the meta-model is created using the Unified Modeling Language (UML). There are 12 components in it.

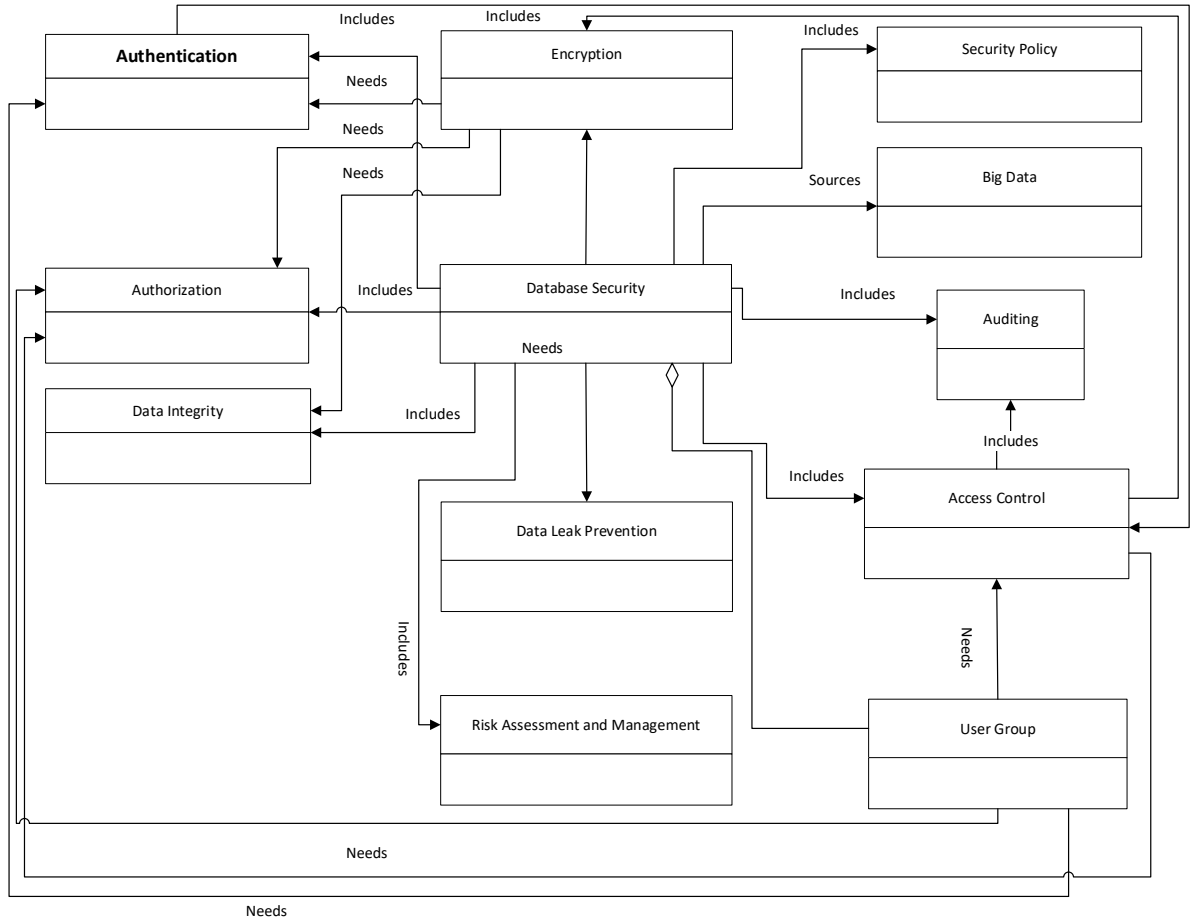

Fig. 3: DBSM

- Step 5. Validating the developed DBSM: The objective of validating a DBSM is to validate that the meta-model is accurate and compatible to user requirements. Validation is critical since it gives a means of measuring the model's quality and efficacy. Additionally, it helps to detect any potential issues or holes in the model, which can then be resolved prior to the model's implementation. By validating a DBSM, developers can ensure the model's dependability, security, and compliance with user needs. Consequently, the developed DBSM may be validated by meta-model modification. The process of modifying a meta-model into another model by mapping one set of components to Kebande and Choo (2022) and Kebande et al. (2022). The subsequent paragraphs provide further details regarding meta-model transformation. Fig. 4 depicts the modification of the meta-model.

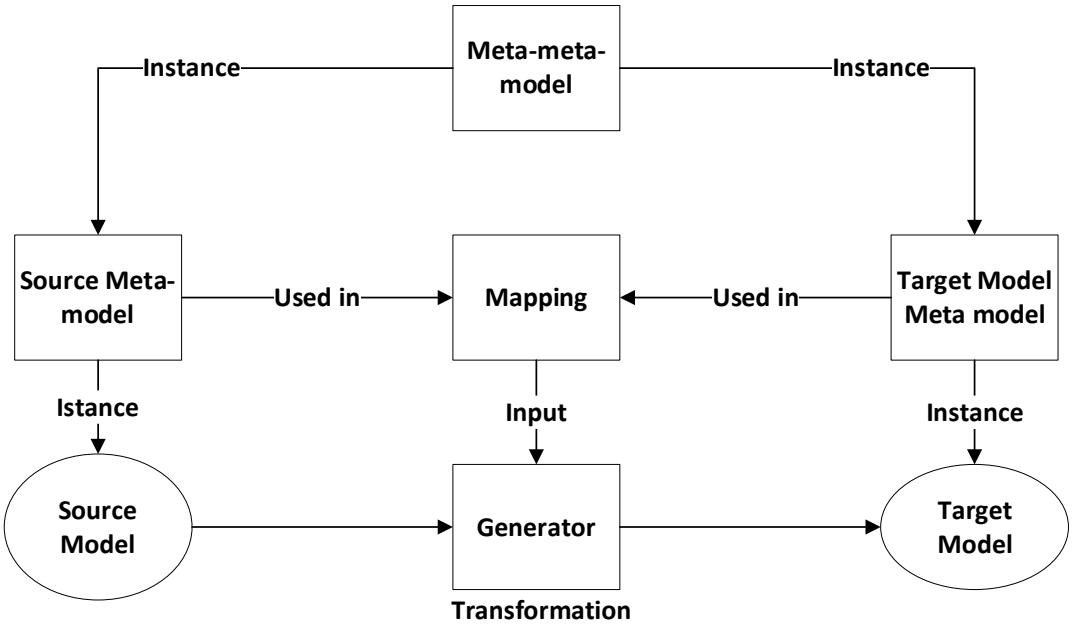

Fig. 4: Meta-model transformation (Makura et al., 2021)

Transformation of meta-models results in the generation of solution models (Martínez-Salvador et al., 2023). Transformation definitions are a set of rules that describe how to move solution models from one meta-model to another. Transform rules describe how to transform one or more components in one meta-model into another (Martínez-Salvador et al., 2023). It is the transformations that are applied to an abstraction hierarchy that determines whether meta-models are practical for use (Kurtev, 2008). The Model-To-Model transformation is an essential tool for deriving engineering and support for understanding our DBSM's various functionality. To have an interoperable database security solution model, the developed DBSM needs to be transformed into several different database security models solutions. To perform the transformation of meta-model-to-model for DBSM, this study follows the methods proposed by Meta Object Facility (MOF). There are two dimensions to model transformation in MOF: vertical and horizontal (Henderson-Sellers, 2011). Transforming a model vertically refers to taking it from one abstraction level to another. As shown in Fig. 5, a transformation can be from an upper to a lower level (e.g., from an M2 meta-model to an M1 or M0 model). A vertical transformation is also used to derive individual components in the models. According to Henderson-Sellers (2011), conformance to a meta-model occurs when a model is specified by the meta-model and used according to its rules. A vertical transformation instantiation and a conformance factor are considered as two aspects of vertical transformation (Alhussan et al., 2022b). A concept is instantiated from the meta-model by instantiating one component, whereas a model object is derived from more than one component by instantiating multiple components from the meta-model (at M2). As both instantiation and conformance belong to the vertical model transformation class, conformance can be seen as one of its more general applications. In this study, the author shows how one or more components in DBSM (at M2) can be used to derive one or more concepts in a model (at M1). DBSM components are usually used at M1 as well as M1 components.

In this study, vertical transformation is achieved by deriving M2-DBSM from its conformant M1-DBS user model and M0-DBS user data model. All three levels of transformation can be horizontal: The User Data level (M0), the User Model level (M1), and the Meta-model level (M2). Model artifacts are typically evaluated in this type of transformation. As the abstraction level of a modeling artifact increases, the semantics of the evaluation also increase.

Model transformations in Object Management Group (OMG) are specified in Query/Views/Transformation (QVT) (Kurtev, 2008). Model transformation is considered one of the most important operations since it is used to manipulate models in a variety of ways. It is designed to

formalize vertical transformations from one model to another model. It focuses on the process and means of going from the source model (meta-model) to the target model (meta-model instance). Therefore, the rules that control the behaviors of the DBSM transformation are adapted from the QVT language. The next subsections explain in detail the DBSM rules and instantiations process, which govern and control the behavior of the DBSM components.

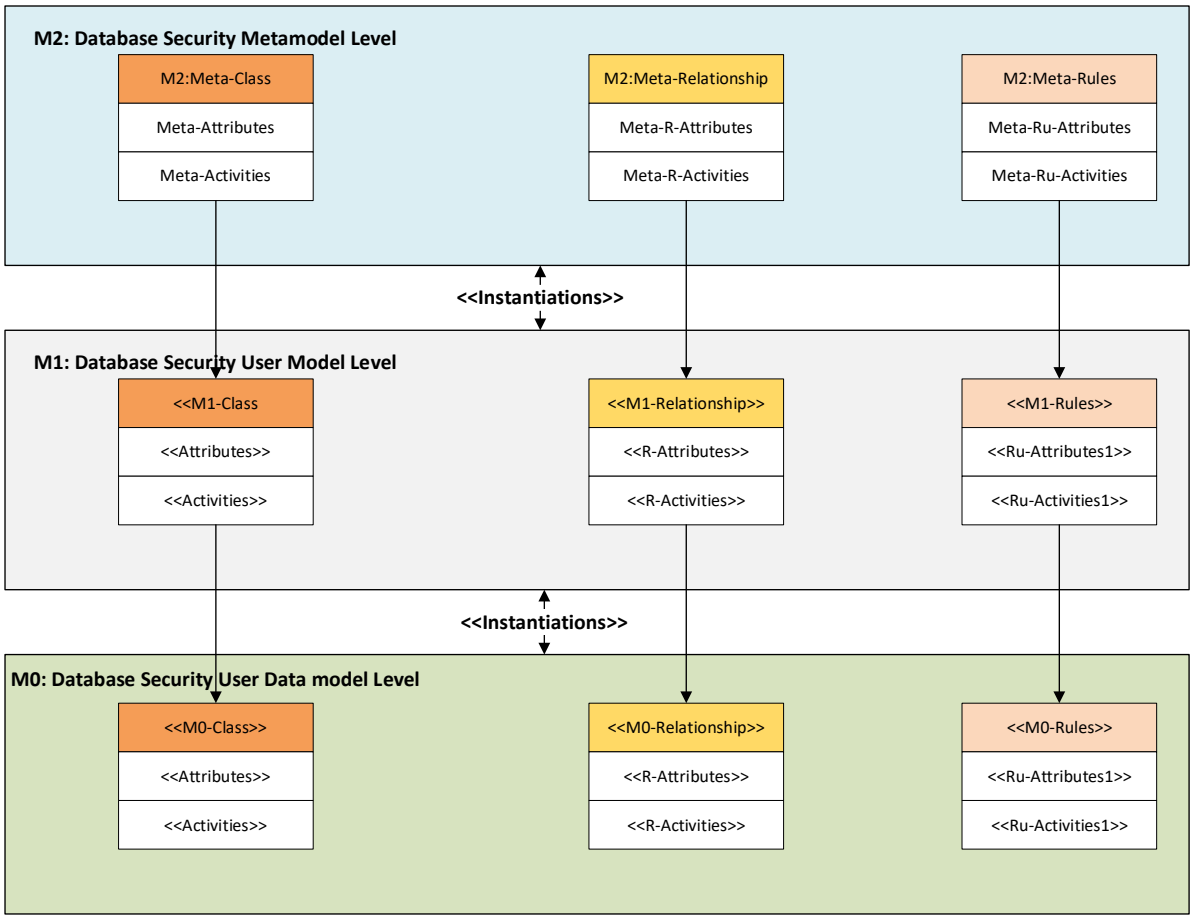

Fig. 5: Instantiation process

a) Adapting Modeling Rules for DBSM: This section introduces a group of rules and guidelines that govern the utilization and behaviors of the DBSM elements. According to Kurtev (2008), the meta-model is usually defined as a set of constructs of a modeling language (components) and their relationships as well as modeling rules. These rules act as policy guidelines for the correct utilization of the DBSM modeling component and agreement of model transformations, as prescribed in [58]. The transformation from a source model (DBSM) to a corresponding target model (either an M1-User Model or an M0-User Data Model) is guaranteed. Therefore, the following examples of DBSM rules consist of:

- Rule_ID (an ID of rule),
- Rule_Name (a name of rule),
- Rule_Syntax (language rule sentence) and,
- Rule_Meaning (a meaning of rule).

To enable users to instantiate/derive solutions from DBSM, three modeling rules are proposed in this study:

- R1- DBMS Components: This rule is used to represent the DBSM components.
- R2- Instance Model of DBSM: This rule is used to create an instance of meta-model (target model from source meta-model DBSM. It ensures each newly created database security model (meta-model instances) is compliant with the DBSM (μDBSM). This rule will mostly be used in association with other rules according to the type of model being developed. The UML Stereotype mechanism (<< >>) is used to help users in the instantiation/derivation process. It's used to generate DBSM-Object from DBSM-Concept or to generate DBSM-Instance from DBSM-Object.
- R3- instantiated model components: This rule is used to govern the components of the instantiated model (instance of DBSM). It ensures that the instantiated model has only the components and their relationships from the DBSM. Based on R3, several specific models can be instantiated from the DBSM. Examples of these models include access control models, data encryption models, data integrity models, and data auditing models. The next section explains the implementation of the developed DBSM in the real scenarios of the database security context.

Rule_ID: R1
Rule_Name: DBSM Concepts
Rule_Syntax: CM (μDBSM) where CM ∈ meta-model concepts: = [Database Security, Authentication, Authorization, Access Control, Encryption, Editing, Security Policy, Data Integrity, Big Data, User Group, Risk Assessment and Management, Data Leak Prevention.
Rule_Meaning: Database Security Meta-model Concepts

Rule_ID: R2
Rule_Name: Instance/Derive Model of DBSM
Rule_Syntax: (μDBSMTarget =< μDBSMSource) if:
(a) Γ′ (μDBSMTarget = Γ′ (μDBSMSource) and
(b) Γ′C (μDBSMTarget ⊆ Γ′C (μDBSMSource).
Rule_Meaning: the derived database security model (target model) is a sub-meta-model if the derived database security model (target model) equal to source meta-model, and the concepts of the derived database security model (target model) are a subset of the source meta-model.

Rule_ID: R3
Rule_Name: instantiated model components
Rule_Syntax: (CM (μDBSMInstantiatedModel) ^ r (CM (μDBSMInstantiatedModel))) ∈ ι (μDBSMInstantiatedModel)
Rule_Meaning: instantiated model must only contain the concepts and their relationships from the DBSM.

b) Instantiation Process: This section discusses the instantiation/derivation process domain practitioners follow to build their solution models based on the suggested modeling rules in the previous section. The instantiation/derivation process includes:

- Identify the target model components that map with the components in the DBSM (source meta-model).
- Identify the relationships between the components of the target model and how they interact.
- Identify the modeling rules that should be applied to the derived components and relationships. For example, to instantiate an M1-Authentication user model (target model) from the source meta-model DBSM, the user should follow these steps:

- Determine which target model components map onto the source meta-model (database security). Five main components have been determined for the M1-Authentication user model (target model) from the DBSM (source meta-model), which are <<Database Security>>, <<Access Control>>, <<User Group>>, <<Authorization>>, and <<Authentication>>.
- Ten (10) relationships have been identified among the determined components.
- Two modeling rules are used to derive the components and relationships, which are R2 and R3.

Rule_ID: R2
Rule_Name: Instance/Derive Authentication User Model from DBSM
Rule_Syntax: (μDBSMAuthentication user model =< μDBSMDBSM) if:
(c) Γ′ (μDBSMAuthentication user model = Γ′ (μDBSMDBSM) and
(d) Γ′C (μDBSMAuthentication user model ⊆ Γ′C (μDBSMDBSM).
Rule_Meaning: instantiated an authentication user model from the DBSM.

Rule_ID: R3
Rule_Name: instantiated authentication user model components
Rule_Syntax: (CM (μDBSM Authentication User Model) ^ r (CM (μDBSM Authentication User Model))) ∈ι (μDBSM Authentication User Model)
Rule_Meaning: the instantiated authentication user model contains the concepts and their relationships from the DBSM.

Therefore, and based on the instantiation process above, Fig. 6 illustrates how the authentication user model is generated from the DBSM. Based on the DBSM, the M1-Authentication user model, which is illustrated in Fig. 6, is a set of components that are derived from the DBSM. The components of the derived model are authentication, authorization, access control, and user groups, which are derived from the DBSM. In the example of verifying the identity of the user, the author finds that this represents the <<Authentication>> component, while grant access represents the <<Authorization>> component, and User represents the <<User Group>> components, and so on. Each component M1-Authentication user model has M1-Attribuets, M1-Activiteis, M1-Realtioship, and M1-Rules.

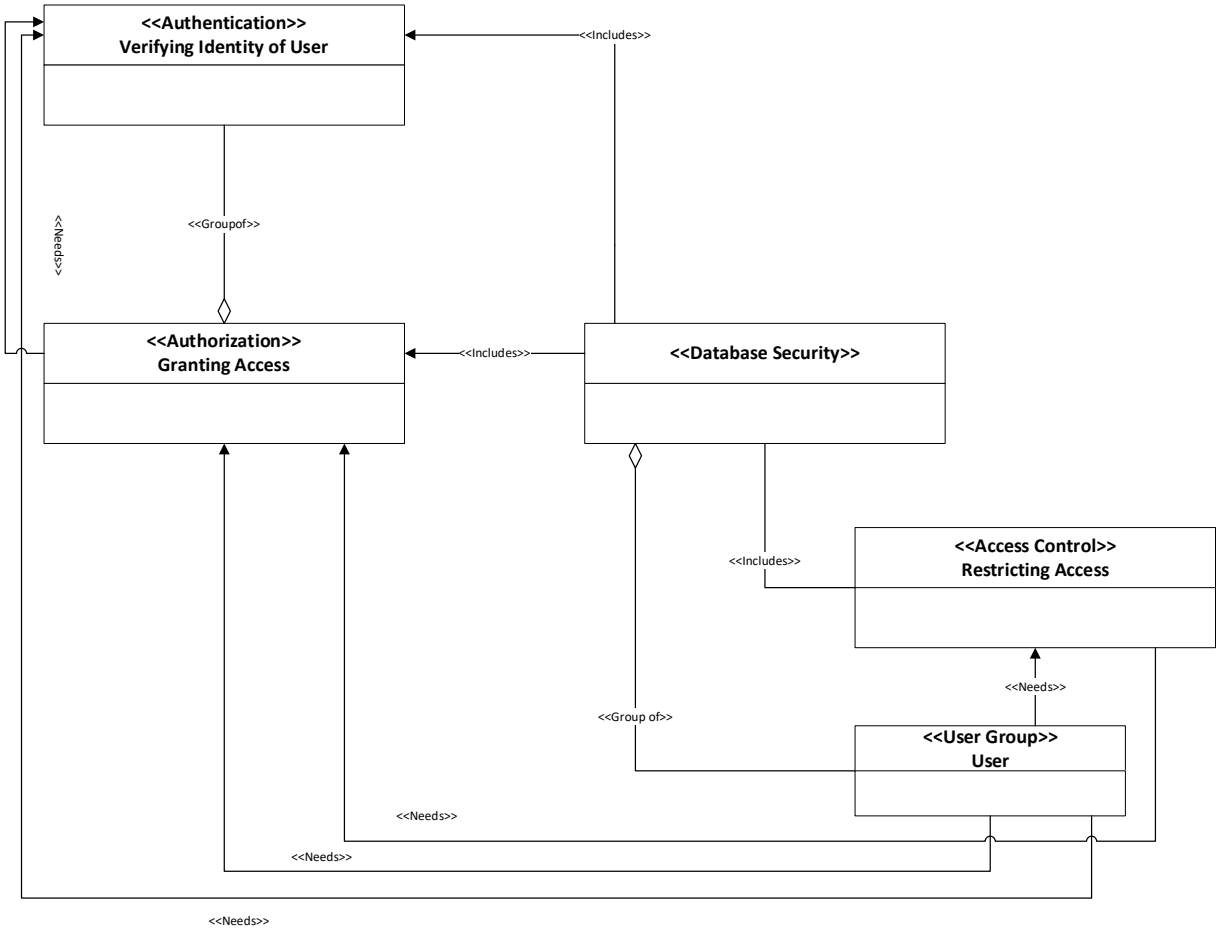

Fig. 6: M1-Authentication user model instantiated from the DBSM

Therefore, the proposed security meta-model can address a variety of scenarios and provide a comprehensive solution for implementing robust security measures for databases. Organizations that handle sensitive or confidential information are examples of this type of scenario. There are several types of online businesses, including financial institutions, government agencies, healthcare providers, and businesses that operate online. We cannot overstate how important it is to safeguard sensitive information in the digital age. Customers' accounts, transactions, and other types of sensitive information regarding their accounts are stored and received by financial institutions. A robust security framework is undoubtedly necessary to prevent unauthorized access, theft, or misuse of this data.

As further evidence of the confidentiality of patient data, healthcare providers also handle highly sensitive, personal, and financial information about their patients. A healthcare organization is responsible for protecting the privacy of its patients, preventing data breaches, and ensuring that robust security measures are in place. HIPAA (Health Insurance Portability and Accountability Act) is strict privacy legislation, so they must comply).

4. Solutions for the research questions

This part gives an explanation about the specified explanations for the research questions emphasized in this study:

1. What are the current database security models?

In this study, various database security models were studied to detect their advantages and disadvantages. There are some security models that emphasize access control, which keeps unauthorized people from accessing the database by restricting access. As a way of safeguarding sensitive information, models use techniques such as encryption. In addition, models emphasize auditing and monitoring to enhance accountability. Additionally, models can be equipped with intrusion detection techniques to detect and respond to potential breaches in security.

2. What are the advantages and disadvantages of the current database security models?

Section 2 provides a detailed explanation of the advantages and disadvantages of the current database security models. These advantages and disadvantages gave the author a solid decision to search for alternative solutions.

3. Is there a meta-model for the database security domain? If yes, what are the advantages and disadvantages of it.

According to our systematic analysis of the existing works in the field of database security, there is a lack of a pure meta-model in this area. As a result

of this lack, security approaches are subject to challenges and limitations because of inconsistency, interoperability, and evaluation. As we move forward, it becomes increasingly critical to address this gap by developing a comprehensive meta-model that will enhance collaboration, knowledge sharing, and the advancement of database security.

5. Results and discussions

This section discusses the results of the study and how they were reached. The author of this study attempts to develop an abstract model to structure and organize the database security domain from the big data perspective, which is called the DBSM. It consists of three levels: M2: DBSM, M1: DBS user model, and M0: DBS user data model level. M2-Level: DBSM includes the abstract components, relationships, and modeling rules as shown in Fig. 7. It includes the 12 abstract components (database security, access control, authentication, authorization, data integrity, encryption, auditing, big data, data leak prevention, user group, risk assessment and management, security policy), relationships and modeling rules. This level provides whole fundamentals to govern the behaviors of the below level (M1: DBS user model). Depending on the requirements of the domain practitioners, the model can be created according to his or her specific needs. For instance, they can identify the specific components with their relationships and then use the proper modeling rules, which allow them to instantiate the M1: DBS user model by first identifying the specific components and their relationships. An example of how the DBSM can be used to derive or create a solution model can be seen in Fig. 7.

On the other hand, the M1: DBS user model level provides a clear description of the steps that should be followed to develop the M0: DBS user data model. The information provided at this level is sufficient for a developer to design a model, make it real, and implement it on the ground. The real attributes, activities, relationships, and modeling rules are provided at this level. Accordingly, the M1-authentication user model, which is instantiated from the DBSM, has a specific set of components, as shown in Fig. 6. It is important to note that these components have attributes, activities, relationships, and rules that govern the behaviors of the lower level M0: DBS user data model. Based on these elements, users can develop the M0: DBS user data model.

DBSM can be considered a novel work that is different from many existing DBS models, as it combines all the existing DBS models, processes, activities, and tasks into one meta-model that has been developed in this study. The DBSM consists of three levels of foreground level: M2-Meta-model Level (DBSM), M1-DBS Model Level, and M0-DBS User Data Model Level, respectively. Fig. 7 depicts each level of the hierarchy as representing or governing the lower layers of the hierarchy. Specifically, M1 is the user model (metadata), M0 is the user data model (data), M2 is the meta-model (meta-metadata), and M3 represents the model. Consequently, domain practitioners can generate/derive their own solution models from the meta-model, thereby implementing the solution once it has been generated. This DBSM has several benefits, which are as follows:

1. The meta-model offers the message among database security through a shared layer that has all duties, perceptions, actions, and procedures for DBS.
2. It offers a theoretical roadmap to enterprise an effective model to accomplish, reprocess, and share the DBS knowledge and data.
3. It is simply appropriate, especially for the DBS experts, to scheme and make new answers by using all the characteristics and processes based on the meta-model necessities.
4. It offers rapid access to DBS knowledge and aids in designing new solutions.

In conclusion, the developed DBS) has provided a structured framework that outlines the security requirements and offers a set of components. These components can be used by domain practitioners to develop their own models to meet these requirements. Furthermore, the meta-model allows practitioners to quickly and easily identify critical security needs and create tailored solution models based on these requirements. An additional advantage of using the meta-model is that it facilitates the definition of security policies and procedures to protect the database system based on the components of the meta-model. In essence, the meta-model provides an organized method for developing security solutions, ensuring a comprehensive and standardized approach to address all necessary security measures to safeguard the database system and its data.

Based on the diagram in Fig. 7, the hierarchical relationship between the levels of the organization is shown in the diagram. The hierarchy in Fig. 7 indicates that each level represents or governs the lower layer, illustrating a clear line of hierarchy and interdependency. M2 represents the meta-model, also called meta-metadata, at the top of the hierarchy. This layer defines a user model (M1) and a user data model (M0) to describe the structure and rules for creating those two models. As a framework for generating and invoking solutions, it establishes a framework around which the entire system can be built. Overall, Fig. 7 illustrates how levels in the hierarchy are interconnected and how each level builds on the one below it, demonstrating the interconnectedness of the levels in the hierarchy. To address the unique needs of different domains, this layered approach allows for flexibility, customization, and scalability in developing solutions that are flexible, customized, and scalable.
Comparatively to existing works, the DBSM is a comprehensive model that covers all aspects of a

domain. Table 5 displays the comparison between the DBSM and existing works. Clearly, it was very evident that the DBSM covered the whole domain model in a very comprehensive manner.

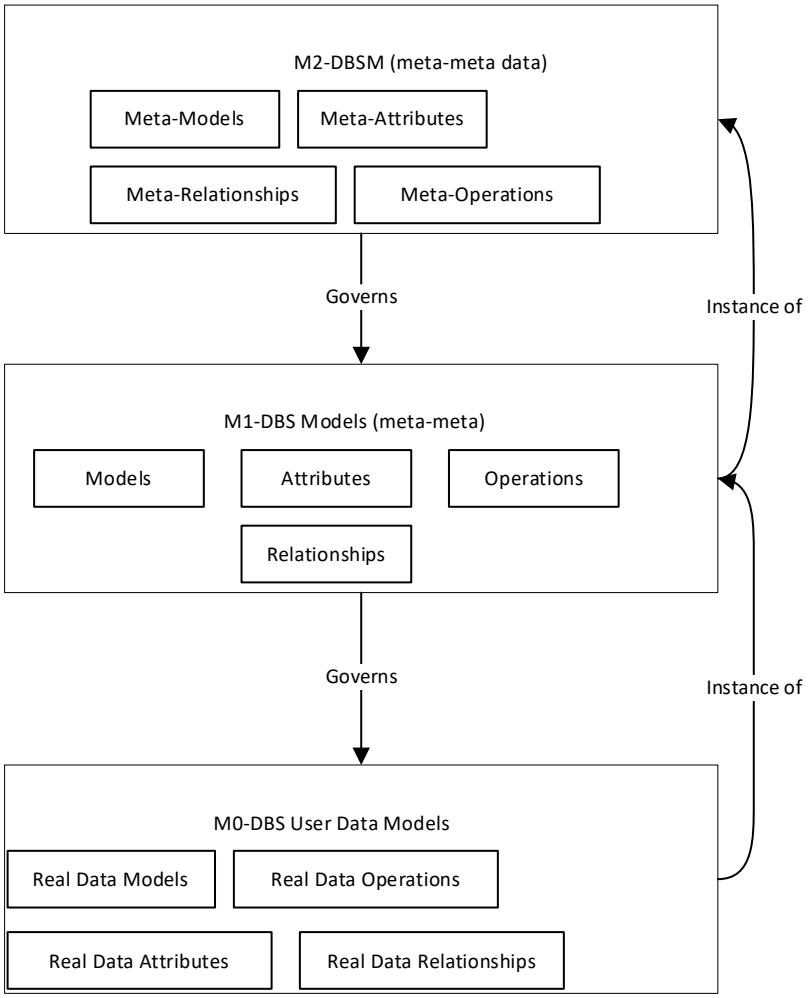

Fig. 7: DBSM levels

Table 5: Comparison between the DBSM and the existing works

Existing works	1	2	3	4	5	6	7	8	9	Developed DBSM
Access control	√	√	√	√	√	√	√	√	√	√
Encryption	×	√	√	√	√	×	×	√	×	√
Decryption	×	√	√	√	√	×	×	√	×	√
Preservation	√	√	√	√	√	√	×	√	√	√
Protection	×	×	√	√	√	×	×	√	√	√
Firewall	×	×	√	√	×	×	×	×	×	√
Data integrity	×	×	×	×	×	×	×	×	×	√
Repudiations	×		×	×	×	×	×	×	×	√
Authorization	×	√	√	×	×	×	×	×	×	√
Authentication	×	×	×	×		√	√	√		√
Data mask	×	×	×	×	×	×	×	×	×	√
Data threats	√	√		×	×	×	×	×	×	√
User identify	×	×	√	√	√	√	√			√
Database protection	×					√	√	√	√	√
Database security policy	×	√	√	√	√		√	√		√
Risk control	×	√	√	√	×	×	×	×	×	√
Risk analysis	×	√	√	√	×	×	×	×	×	√
Assess vulnerabilities	×	×	×	×	√	√	√	√	√	√

1: Albalawi, 2018; 2: Khan et al., 2018; 3: Odirichukwu and Asagba, 2017; 4: Gruschka et al., 2018; 5: Zhang, 2018; 6: Al-Dwairi et al., 2018; 7: Adedayo and Olivier, 2014; 8: Awadallah et al., 2021; 9: Liu et al., 2020

6. Conclusion

Database security can be defined as the prevention and management of malicious intrusions and any efforts with malicious intent directed toward database security. Many different database security models and frameworks have been proposed in the literature over the years to address database security issues. There are also procedures, policies, and techniques that have been proposed. Even so, many aspects of database security were not adequately addressed by these models and frameworks. Thus, database security professionals are working in a diversified, heterogeneous, disorganized, and ambiguous field that is distinguished by its diversity and heterogeneity. In this work, the DBSM has been constructed as a

unified view of the database security domain, which may also be viewed as a language for comprehending the database security domain. The developed DBSM consists of twelve (12) components: Database encryption, access control, database authentication, database authorization, database security policy, database leak prevention, database auditing, risk assessment and management, database integrity, database security, and big data. According to the results of the investigation, the DBSM is competent in developing a solution model to solve its limitations. Hence, future work includes the validation of the applicability and effectiveness of the proposed DBSM to the real world.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Adedayo OM and Olivier M (2014). Schema reconstruction in database forensics. In: Peterson G and Shenoi S (Eds.), Advances in digital forensics X: DigitalForensics 2014: IFIP Advances in information and communication technology: 101-116. Springer, Berlin, Germany.

Albalawi U (2018). Countermeasure of statistical inference in database security. In the IEEE International Conference on Big Data, IEEE, Seattle, USA: 2044-2047. https://doi.org/10.1109/BigData.2018.8622241

Al-Dhaqm A, Abd Razak S, Dampier DA, Choo KKR, Siddique K, Ikuesan RA, and Kebande VR (2020b). 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, Ikuesan RA, Kebande VR, and Siddique K (2020a). A review of mobile forensic investigation process models. IEEE Access, 8: 173359-173375. https://doi.org/10.1109/ACCESS.2020.3014615

Al-Dhaqm A, Abd Razak S, Siddique K, Ikuesan RA, and Kebande VR (2020c). 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, Othman SH, Yafooz WMS, and Ali A (2023a). Review of information security management frameworks. In: Yafooz WMS, Al-Aqrabi H, Al-Dhaqm A, and Emara A (Eds.), Kids cybersecurity using computational intelligence techniques: 69-80. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-21199-7_5

Al-Dhaqm A, Razak S, Ikuesan RA, Keband RV, and Hajar Othman S (2021). Face validation of database forensic investigation metamodel. Infrastructures, 6(2): 13. https://doi.org/10.3390/infrastructures6020013

Al-Dhaqm A, Yafooz WM, Othman SH, and Ali A (2023b). Database forensics field and children crimes. In: Yafooz WMS, Al-Aqrabi H, Al-Dhaqm A, and Emara A (Eds.), Kids cybersecurity using computational intelligence techniques: 81-92. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-21199-7_6

Al-Dwairi RM, Al-Tweit N, and Zyout K (2018). Factors influencing cloud-computing adoption in small and medium e-commerce enterprises in Jordan. In the 2018 1st International Conference on Internet and e-Business, Association for Computing Machinery, Singapore, Singapore: 73-78. https://doi.org/10.1145/3230348.3230370

Alhazmi HE, Eassa FE, and Sandokji SM (2022). Towards big data security framework by leveraging fragmentation and blockchain technology. IEEE Access, 10: 10768-10782. https://doi.org/10.1109/ACCESS.2022.3144632

Alhussan AA, Al-Dhaqm A, Yafooz WM, Emara AHM, Bin Abd Razak S, and Khafaga DS (2022a). A unified forensic model applicable to the database forensics field. Electronics, 11(9): 1347. https://doi.org/10.3390/electronics11091347

Alhussan AA, Al-Dhaqm A, Yafooz WM, Razak SBA, Emara AHM, and Khafaga DS (2022b). Towards development of a high abstract model for drone forensic domain. Electronics, 11(8): 1168. https://doi.org/10.3390/electronics11081168

Ali A, Razak SA, Othman SH, and Mohammed A (2015). Towards adapting metamodeling approach for the mobile forensics investigation domain. In the International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia: 364-368.

Ali A, Razak SA, Othman SH, and Mohammed A (2018). Extraction of common concepts for the mobile forensics domain. In: Saeed F, Gazem N, Patnaik S, Saed Balaid A, and Mohammed F (Eds.), Recent trends in information and communication technology: Proceedings of the 2nd international conference of reliable information and communication technology: 141-154. Springer, Cham, Switzerland.

Alshammari A (2023a). A novel security framework to mitigate and avoid unexpected security threats in Saudi Arabia. Engineering, Technology and Applied Science Research, 13(4): 11445-11450. https://doi.org/10.48084/etasr.6091

Alshammari A (2023b). Detection and investigation model for the hard disk drive attacks using FTK imager. International Journal of Advanced Computer Science and Applications, 14(7): 767-774. https://doi.org/10.14569/IJACSA.2023.0140784

Awadallah R, Samsudin A, Teh JS, and Almazrooie M (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. IEEE Access, 9: 69513-69526. https://doi.org/10.1109/ACCESS.2021.3077123

Chaudhary P, Gupta BB, Chang X, Nedjah N, and Chui KT (2021). Enhancing big data security through integrating XSS scanner into fog nodes for SMEs gain. Technological Forecasting and Social Change, 168: 120754. https://doi.org/10.1016/j.techfore.2021.120754

George G, Osinga EC, Lavie D, and Scott BA (2016). Big data and data science methods for management research. Academy of Management Journal, 59(5): 1493-1507. https://doi.org/10.5465/amj.2016.4005

Gruschka N, Mavroeidis V, Vishi K, and Jensen M (2018). Privacy issues and data protection in big data: A case study analysis under GDPR. In the IEEE International Conference on Big Data, IEEE, Seattle, USA: 5027-5033. https://doi.org/10.1109/BigData.2018.8622621

Henderson-Sellers B (2011). Bridging metamodels and ontologies in software engineering. Journal of Systems and Software, 84(2): 301-313. https://doi.org/10.1016/j.jss.2010.10.025

Kebande V and Venter H (2016). Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. In the 11th International Conference on Cyber Warfare and Security, Boston, USA: 399-406.

Kebande VR and Choo KKR (2022). Finite state machine for cloud forensic readiness as a service (CFRaaS) events. Security and Privacy, 5(1): e182. https://doi.org/10.1002/spy2.182

Kebande VR and Ray I (2016). A generic digital forensic investigation framework for Internet of Things (IoT). In the IEEE 4th International Conference on Future Internet of Things and Cloud, IEEE, Vienna, Austria: 356-362. https://doi.org/10.1109/FiCloud.2016.57

Kebande VR, Ikuesan RA, and Karie NM (2022). Review of blockchain forensics challenges. In: Baalamurugan K, Kumar SR, Kumar A, Kumar V, and Padmanaban S (Eds.), Blockchain security in cloud computing: 33-50. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-70501-5_3

Kebande VR, Ikuesan RA, Karie NM, Alawadi S, Choo KKR, and 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

Khan MI, O'Sullivan B, and Foley SN (2018). Towards modelling insiders behaviour as rare behaviour to detect malicious RDBMS access. In the IEEE International Conference on Big Data, IEEE, Seattle, USA: 3094-3099. https://doi.org/10.1109/BigData.2018.8622047

Kulkarni S and Urolagin S (2012). Review of attacks on databases and database security techniques. International Journal of Emerging Technology and Advanced Engineering, 2(11): 253-263.

Kurtev I (2008). State of the art of QVT: A model transformation language standard. In: Schürr A, Nagl M, and Zündorf A (Eds.), Applications of graph transformations with industrial relevance: Lecture notes in computer science: 377-393. Springer, Berlin, Germany. https://doi.org/10.1007/978-3-540-89020-1_26

Lessambo FI (2023). The cybersecurity counteroffensive. In: Lessambo FI (Ed.), Anti-money laundering, counter financing terrorism and cybersecurity in the banking industry: A comparative study within the G-20: 11-32. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-23484-2_2

Liu Q, Peng Y, Pei S, Wu J, Peng T, and Wang G (2020). Prime inner product encoding for effective wildcard-based multi-keyword fuzzy search. IEEE Transactions on Services Computing, 15(4): 1799-1812. https://doi.org/10.1109/TSC.2020.3020688

Makura S, Venter HS, Kebande VR, Karie NM, Ikuesan RA, and Alawadi S (2021). Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring. Security and Privacy, 4(3): e149. https://doi.org/10.1002/spy2.149

Martínez-Salvador B, Marcos M, Palau P, and Mafé ED (2023). A model-driven transformation approach for the modelling of processes in clinical practice guidelines. Artificial Intelligence in Medicine, 137: 102495. https://doi.org/10.1016/j.artmed.2023.102495 **PMid:36868689**

Ngadi M, Al-Dhaqm R, and Mohammed A (2012). Detection and prevention of malicious activities on RDBMS relational database management systems. International Journal of Scientific and Engineering Research, 3(9): 1-10.

Odirichukwu JC and Asagba PO (2017). Security concept in Web database development and administration: A review perspective. In the IEEE 3rd International Conference on Electro-Technology for National Development, IEEE, Owerri, Nigeria: 383-391. https://doi.org/10.1109/NIGERCON.2017.8281910

Ratner B (2003). Statistical modeling and analysis for database marketing: Effective techniques for mining big data. CRC Press, Boca Raton, USA.

Saleh M, Othman SH, Driss M, Al-dhaqm A, Ali A, Yafooz WM, and Emara AHM (2023). A metamodeling approach for IoT forensic investigation. Electronics, 12(3): 524. https://doi.org/10.3390/electronics12030524

Saleh MA, Othman SH, Al-Dhaqm A, and Al-Khasawneh MA (2021). Common investigation process model for Internet of Things forensics. In the 2nd International Conference on Smart Computing and Electronic Enterprise, IEEE, Cameron Highlands, Malaysia: 84-89. https://doi.org/10.1109/ICSCEE50312.2021.9498045 **PMid:34022883 PMCid:PMC8140497**

Salem M, Othman SH, Al-Dhaqm A, and Ali A (2023). Development of metamodel for information security risk management. In: Yafooz WMS, Al-Aqrabi H, Al-Dhaqm A, and Emara A (Eds.), Kids cybersecurity using computational intelligence techniques: 243-253. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-21199-7_17

Tall AM and Zou CC (2023). A framework for attribute-based access control in processing big data with multiple sensitivities. Applied Sciences, 13(2): 1183. https://doi.org/10.3390/app13021183

Teimoor RA (2021). A review of database security concepts, risks, and problems. UHD Journal of Science and Technology, 5(2): 38-46. https://doi.org/10.21928/uhdjst.v5n2y2021.pp38-46

Ullah F, Pun CM, Kaiwartya O, Sadiq AS, Lloret J, and Ali M (2023). HIDE-Healthcare IoT data trust management: Attribute centric intelligent privacy approach. Future Generation Computer Systems, 148: 326-341. https://doi.org/10.1016/j.future.2023.05.008

Wąsowski A and Berger T (2023). Model and language variability. In: Wąsowski A and Berger T (Eds.), Domain-specific languages: Effective modeling, automation, and reuse: 459-486. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-23669-3_13

Yafooz WM, Bakar ZBA, Fahad SA, and Mithun MA (2020). Business intelligence through big data analytics, data mining and machine learning. In: Sharma N, Chakrabarti A, and Balas V (Eds.), Data management, analytics and innovation: proceedings of ICDMAI 2019: 217-230. Volume 2, Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-13-9364-8_17

Yaseen Q, Jararweh Y, Panda B, and Althebyan Q (2017). An insider threat aware access control for cloud relational databases. Cluster Computing, 20: 2669-2685. https://doi.org/10.1007/s10586-017-0810-y

Zhang D (2018). Big data security and privacy protection. In the 8th International Conference on Management and Computer Science, Atlantis Press, Shenyang, China: 275-278. https://doi.org/10.2991/icmcs-18.2018.56