e-ISSN: 3124-6788	SADANA: International Journal of Education, Law, Technology, Economics and Agriculture: Volume: 1, Number: 1, (2026), Page: 109-123

Research Article

The Sattar Al-'Uyub Principle in Data Privacy Architecture: An Ethical Analysis of Centralized Databases

Rifki Maulana: Muhammadiyah University of Sukabumi, **Indonesia**; Email: rifki.maulana@ummi.ac.id
Iqbal Noor: Muhammadiyah University of Sukabumi, **Indonesia**; iqnoor@ummi.ac.id
*Corresponding Author: rifki.maulana@ummi.ac.id
DOI: | received: 02-18-2026; accepted: 02-28-2026; online: 03-29-2026

Abstract: *The development of centralized database architectures in the digital era raises various issues related to data privacy, cybersecurity, and the ethics of personal information management. Centralized database systems offer high efficiency in data integration and management, but also pose serious risks such as data leakage, unauthorized access, and digital surveillance. This study aims to analyze the relevance of the Sattar al-'Uyub principle in the ethics of data privacy and centralized database governance. The study uses a Systematic Literature Review (SLR) approach with the PRISMA 2020 framework and the PICOS model to systematically identify, evaluate, and synthesize scientific literature for the period 2020–2026. A total of 51 selected articles were analyzed using a thematic approach. The results show that modern data security studies are still dominated by technical approaches, while ethical and spiritual dimensions are still relatively limited. The Sattar al-'Uyub principle, which emphasizes the protection of individual honor, confidentiality, and concealment, has strong relevance as an ethical foundation in modern digital data governance. This study provides a conceptual contribution through the integration of Islamic information ethics with database security architectures such as Transparent Data Encryption (TDE), Role-Based Access Control (RBAC), and ethics-based data governance. The study concluded that protecting digital privacy requires a combination of technological security and a strong moral foundation.*

Keywords: Sattar Al-'Uyub, Data Privacy, Centralized Database, Islamic Ethics and Cyber Security.

1. Introduction

The development of information and communication technology in the digital era has brought fundamental changes in human interaction patterns, organizational governance, and information storage and distribution mechanisms. Digital transformation has encouraged government institutions, companies, educational institutions, hospitals, the financial sector, and digital platforms to rely on database systems to manage massive amounts of public data. Centralized database architecture has become the dominant model because it offers high efficiency in data integration, ease of system control, accelerated information access, and optimization of data-driven decision-making. This system allows all user data to be concentrated in a single management center, simplifying synchronization and monitoring of organizational operations.

Amid the increasing use of centralized databases, serious issues regarding data security and privacy have emerged. People's personal data has become a valuable economic asset, exploited for various business, political, digital marketing, and artificial intelligence (AI) development purposes. Personal information such as identity, health records, financial transactions, geographic location, behavioral preferences, and individual digital activities is continuously collected by various digital platforms. This phenomenon demonstrates that modern humans live in an increasingly complex and difficult-to-control digital surveillance ecosystem (Zuboff, 2021).

This situation is exacerbated by the increasing number of personal data breaches in various countries, including Indonesia. Data breaches in both public and private institutions demonstrate that centralized database systems are highly vulnerable to cyberattacks, internal misuse, weak access

controls, and commercial exploitation of user data. In some cases, public data is traded without the explicit consent of the information owner. This situation poses a serious threat to the right to privacy, individual security, and the protection of human dignity in the digital space. Data privacy issues are no longer merely related to the technical aspects of system security but have evolved into issues of ethics, power, and humanity.

Contemporary studies on digital privacy show that data control by certain institutions creates an unequal relationship between users and system administrators. Individuals often lose control of their personal data once it enters a digital system. Centralized database models allow organizations to exert significant capacity for surveillance, behavioral analysis, and predicting individual decisions through big data analytics and artificial intelligence algorithms. This situation gives rise to the phenomenon of surveillance capitalism, the practice of exploiting human data for economic gain and social control (Zuboff, 2021).

A modern technology ethics perspective views privacy as a fundamental human right related to freedom, dignity, and the protection of personal identity. Privacy violations can lead to serious social and psychological impacts, such as behavioral manipulation, digital discrimination, identity theft, and even damage to an individual's reputation. Therefore, various countries have begun strengthening personal data protection regulations in response to increasing information security threats. The European Union, through its General Data Protection Regulation (GDPR), is one example of a global regulation that places privacy protection as part of digital human rights (European Data Protection Board, 2024). Indonesia has also passed the Personal Data Protection Law as an effort to strengthen national data governance.

Despite the continued development of security regulations and technology, numerous data breaches continue to occur. This demonstrates that addressing digital privacy issues through technical and legal approaches alone is not sufficient. The underlying problem lies in the weak ethical foundations in the design and governance of information systems. Many organizations still view user data as merely an economic object, without considering the moral value of its management. Modern cybersecurity approaches generally focus on encryption, authentication, and system controls, but have not yet addressed the moral responsibility to protect the dignity of human data owners.

In this context, an Islamic ethical approach offers an important and relevant perspective for study. Islam, as a comprehensive religion, not only regulates humanity's spiritual relationship with God but also establishes moral principles for safeguarding the rights, honor, and privacy of others. One principle strongly relevant to digital privacy issues is the concept of Sattar al-'Uyub. Terminologically, this concept refers to the behavior of concealing shame, maintaining confidentiality, and protecting individual honor from the dissemination of information that could harm human dignity. This principle is rooted in Islamic values of compassion, social protection, and respect for personal rights.

In Islamic tradition, maintaining individual confidentiality and honor is an essential part of social ethics. The Quran and Hadith contain numerous teachings prohibiting the disclosure of others' secrets, the prohibition of spying, and the obligation to safeguard confidential information. These values demonstrate that Islam had a foundation for privacy ethics long before the emergence of modern concepts of data protection. The relevance of the principle of Sattar al-'Uyub becomes even more crucial in the digital age, when personal data can be widely disseminated within seconds through global information technology systems.

The principle of Sattar al-'Uyub can serve as a normative basis for building a more ethical and humane data privacy architecture. In the context of centralized databases, this principle can be translated into various mechanisms such as restricting data access, minimizing the collection of

personal information, transparency in data use, protecting user confidentiality, and strengthening the moral responsibility of information system managers. This approach broadens the understanding that data protection is not only related to technological security but also concerns the protection of human dignity, which is the core of digital ethics.

The urgency of this research is growing as the development of artificial intelligence, machine learning, the Internet of Things (IoT), and national digital identity technologies leads to increasingly widespread data integration. Centralized database systems allow all individual activities to be digitally documented and automatically analyzed by algorithms. This situation increases the risk of data misuse by states, technology companies, and cybercriminals. Furthermore, the concentration of data in a single system also creates structural risks in the form of information monopolies and the dominance of digital power by certain institutions (Floridi, 2023).

Research on data privacy has been largely dominated by Western approaches focused on individual rights, legal regulations, and system security. Studies integrating Islamic ethical principles into database architecture design are relatively limited. This is despite the fact that Muslims constitute one of the largest groups of digital technology users worldwide. This lack of research demonstrates the academic need to develop a digital ethics paradigm based on Islamic values that can address contemporary technological challenges.

The novelty of this research lies in its attempt to integrate the principle of Sattar al-'Uyub as an ethical framework in the analysis of centralized database architecture. This article not only discusses data privacy from an information security perspective but also develops a normative approach that places the protection of human dignity as the primary orientation of technology design. This research offers a new perspective that modern database governance should not only be technically efficient but also fulfill moral and spiritual responsibilities towards system users.

In addition to providing theoretical contributions to the development of Islamic technology ethics, this research also has practical implications for information system developers, policymakers, government institutions, technology companies, and academics. The principle of Sattar al-'Uyub can be used as a basis for designing data protection policies, information security governance, and the development of digital technologies that are more equitable and oriented towards human protection. Thus, this article seeks to present a synthesis of Islamic values and the challenges of modern technology in building an ethical, secure, and sustainable digital ecosystem.

2. Literature Review

Centralized Database Architecture and Privacy Risks

A centralized database architecture is a data storage model that places all information in a single, integrated management center. This model is widely used because it improves operational efficiency, data consistency, ease of administration, and speeds organizational decision-making. In digital government systems, healthcare, banking, education, and e-commerce, centralized databases are a key infrastructure supporting real-time information exchange (Elmasri & Navathe, 2021).

Despite offering high efficiency, data centralization creates significant security risks. Concentrating information in a single storage center leaves the system vulnerable to cyberattacks, data theft, ransomware, and internal access abuse. According to research by Alhassan and Mahmood (2022), centralized databases have a structural weakness in the form of a single point of failure, where a single point of failure can disrupt the entire organization's information system. This risk is exacerbated when organizations manage large amounts of sensitive data without a robust access control system.

Recent research shows that modern database security threats stem not only from external hackers but also from poor data governance practices. Kim, Wang, and Park (2023) explain that many institutions fail to implement the principle of least privilege access, resulting in internal users having excessive access to sensitive information. This situation increases the potential for data breaches due to human error and abuse of authority.

Contemporary information security studies also highlight that centralized databases are often primary targets in the global cybercrime ecosystem. According to a study by Rao and Vemuri (2021), attacks on data centers have increased significantly since the rise of cloud-based services and big data integration. Attackers not only seek economic gain but also exploit data for political manipulation, social surveillance, and the exploitation of people's digital behavior.

Another perspective is put forward by Chen and Li (2024), who state that the development of artificial intelligence is expanding organizations' capacity to conduct in-depth personal data analysis. Data stored in centralized databases can be used to predict individual behavior, consumption preferences, and even political leanings. This situation raises concerns about the loss of privacy autonomy and the increasing dominance of institutions over people's digital lives.

In the context of modern governance, data protection can no longer rely solely on firewalls and traditional authentication systems. Data-centric security approaches are being developed to ensure that protection is inherently embedded in the information being stored. This approach includes encryption, tokenization, adaptive access control, and periodic data usage audits (NIST, 2023). This security model demonstrates that digital privacy must be understood as an integral part of information system architecture design.

Islamic Information Ethics and the Concept of Sattar al-'Uyub

Islamic information ethics views personal information as an integral part of human dignity that must be protected. In Islam, keeping secrets and covering up the faults of others is not only a social act, but also a moral and spiritual obligation. The concept of Sattar al-'Uyub stems from divine values that emphasize the protection of individual honor by prohibiting the disclosure of someone's faults, secrets, or weaknesses without a justifiable reason according to Islamic law.

Rahman's (2021) study explains that the concept of privacy in Islam has broader dimensions than modern secular approaches. Privacy relates not only to an individual's right to personal data but also to the protection of human dignity. Therefore, the unauthorized dissemination of sensitive information is seen as an ethical violation that can undermine social relationships and human values.

The principle of Sattar al-'Uyub is also closely related to the prohibition of tajassus, which is the unauthorized search for faults or personal information of others. According to research by Al-Qaradawi and Hasan (2022), the prohibition of tajassus in Islam can serve as a normative basis for developing modern digital data collection ethics. Excessive tracking of user data without consent is considered contrary to Islamic principles of privacy protection.

In the context of digital technology, the concept of Sattar al-'Uyub provides a new perspective on the moral responsibility of information system developers. Yusuf and Ibrahim (2023) state that database managers have an ethical mandate to ensure that user information is not used exploitatively. Data protection must be understood as part of digital ethics that places human security and dignity above economic interests.

Ahmed and Saeed's (2024) research shows that Islamic information ethics can contribute to the development of a more equitable data governance model. An information system based on Islamic values emphasizes transparency, honesty, restricted access, and social responsibility in information

management. This approach differs from the paradigm of digital capitalism, which often treats user data as an economic commodity.

Cyber Security in the Frame of Maqasid al-Shari'ah

The concept of Maqasid al-Shari'ah provides an important philosophical framework for understanding cyber security from an Islamic perspective. The main aim of Islamic law is to protect religion (hifz al-din), soul (hifz al-nafs), reason (hifz al-'aql), descendants (hifz al-nasl), and property (hifz al-mal). In the modern digital context, the protection of personal data can be linked to the protection of an individual's life, honor and property.

According to research by Farooq and Abdullah (2021), digital identity in the modern era is a personal asset that must be protected. Data breaches can lead to financial loss, social manipulation, and even psychological harm to victims. Therefore, cybersecurity in Islam is viewed not only as a technical safeguard but also as part of the moral responsibility to safeguard human well-being.

Hassan and Karim's (2022) study emphasized that the development of information security systems must adhere to the principles of justice and the protection of individual rights. From the perspective of Maqasid al-Shari'ah, technology should be used to create social benefits (maslahah) and prevent harm (mafsadah). Database systems that are vulnerable to data breaches are considered contrary to the goal of human protection under Islamic law.

Other research by Noor and Ali (2023) shows that the concept of Islamic cybersecurity ethics is highly relevant in addressing the threat of surveillance technology. Massive data collection without ethical controls can create power imbalances and violate people's privacy rights. Islam views that power over information must be limited by the principles of trust and moral responsibility.

Transparent Encryption and Key Management Mechanism

Privacy protection in modern database systems requires robust and adaptive security mechanisms. One key technology used is Transparent Data Encryption (TDE), an automatic encryption method that protects data at rest. This technology ensures data remains protected even in the event of hardware theft or unauthorized access to database files (Oracle Corporation, 2024).

Singh and Patel's (2022) research explains that implementing AES-256 encryption has become the gold standard in modern database protection due to its high level of security and good computational efficiency. This encryption helps prevent unauthorized parties from reading sensitive data.

In addition to encryption, key management systems are a crucial element of database security. According to García and Moreno (2023), the primary weakness in many security systems lies not in the encryption algorithm, but in poor access key management. Therefore, organizations need to implement layered access controls and regular security audits to maintain data integrity.

From an Islamic ethical perspective, the use of encryption technology can be understood as an implementation of the value of protecting human dignity. Technology serves not only as a technical tool but also as a moral instrument for safeguarding the confidentiality of user information. The integration of technological security and Islamic ethics results in a more holistic approach to data protection, placing humans at the center of information system design.

Framework of Thinking

The research framework is a conceptual representation used to explain the relationships between variables in the study. This framework is built on the integration of Islamic ethical perspectives and modern information system security technical approaches in the context of data privacy protection in

a centralized database architecture. This research starts from the assumption that the problem of data leakage and weak digital privacy protection is not only caused by technological weaknesses, but also influenced by a weak ethical foundation in information governance. In this study, Islamic ethical principles are positioned as independent variables that serve as a normative basis for digital data management. The concept of Sattar al-'Uyub, the prohibition of tajassus (espionage), and the value of trust in safeguarding information are seen as fundamental values that can form a more humane and responsible data protection paradigm. These principles are then implemented through a technical approach in the form of database security architecture, such as Transparent Data Encryption (TDE), Dynamic Data Masking (DDM), and Role-Based Access Control (RBAC). The relationships between variables in this study can be illustrated through the following research paradigm.

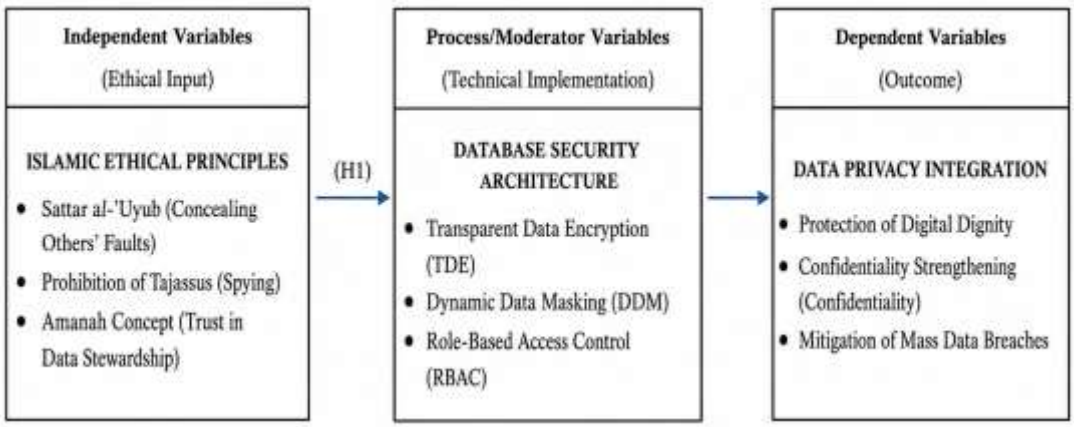

Figure 1. Research Paradigm

Figure 1 illustrates a research paradigm that integrates theological dimensions into a technical framework. This framework begins with the internalization of the principle of Sattar al-'Uyub as the ethical foundation for system development. This value is then transformed into technical policy through three main pillars of database architecture:

1. Transparent Encryption (TDE) as a manifestation of the 'Digital Hijab' to protect data while in storage.
2. Dynamic Data Masking (DDM) is a mitigation measure against acts of tajassus or unauthorized curiosity regarding other people's shame/data.
3. Role-Based Access Control (RBAC) reflects the principle of trust in limiting access rights according to functional needs.

This synergy between ethical values and technical mechanisms is predicted to linearly enhance the integrity of data privacy protection. Thus, information security is no longer viewed as a mere computational burden, but rather as a form of fulfilling human dignity in the digital space.

3. Method

This study uses a Systematic Literature Review (SLR) approach to analyze the Sattar al-'Uyub principle in data privacy architecture and its relevance to centralized database ethics in the digital era. The SLR approach was chosen because it can produce a systematic, transparent, structured, and evidence-based literature synthesis that can provide a deeper conceptual understanding of the integration of Islamic ethics and modern information system security (Snyder, 2019). Through this approach, the study not only identifies the development of data privacy and database security studies but also maps the relationship between Islamic values and contemporary digital data protection practices.

The SLR approach allows researchers to critically evaluate various previous studies on Islamic information ethics, cybersecurity, database governance, digital privacy, and personal data protection. Furthermore, this method helps identify research gaps, current research trends, and opportunities for

developing an Islamic-based technology ethics framework, which remains relatively limited in contemporary academic studies. This research adheres to the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure that the identification, selection, evaluation, and synthesis of articles are conducted objectively and methodologically sound (Page et al., 2021).

In addition to the PRISMA approach, this study also adopted the PICOS (Population, Intervention, Comparison, Outcome, Study Design) framework as an instrument to systematically determine the research focus and article selection criteria. The PICOS framework was used to further direct the literature synthesis process and produce a comprehensive analysis of the relationship between Islamic ethics and data privacy architecture.

a. Identification Stages

The initial stage of the research was carried out through the process of identifying scientific articles relevant to the research topic. A literature search was conducted in various reputable international academic databases such as Scopus, Web of Science (WoS), ScienceDirect, SpringerLink, IEEE Xplore, Emerald Insight, and Google Scholar. The selection of these databases was based on the broad scope of publications in the fields of cybersecurity, technology ethics, information systems, data protection law, and contemporary Islamic studies. This study focused the search for articles during the period 2020–2026 to ensure that the references used were up-to-date and relevant to the latest developments in digital technology. This temporal focus is important because issues of data privacy and database security are evolving rapidly with the increasing use of Artificial Intelligence (AI), cloud computing, big data analytics, and digital identity. The main keywords used in the article search process include:

- "Sattar al-'Uyub" AND "data privacy"
- "Islamic ethics" AND "database security"
- "Islamic information ethics" AND "cybersecurity"
- "centralized database" AND "privacy protection"
- "digital privacy" AND "Islamic perspective"
- "Maqasid al-Shari'ah" AND "data governance"
- "data protection" AND "Islamic ethics"
- "cyber ethics" AND "Islamic values"
- "transparent data encryption" AND "database security"
- "surveillance" AND "Islamic privacy ethics"

Keyword combinations were performed using Boolean operators such as AND and OR to broaden the search scope and increase the relevance of the articles obtained. This search strategy was crucial to ensure that the collected literature was truly relevant to the research focus on data privacy ethics from an Islamic perspective and the implementation of modern database security.

b. Article Selection Stage

The article selection process was conducted based on the PRISMA 2020 procedure, which consists of four main stages: identification, screening, eligibility, and inclusion. During the identification stage, researchers identified 247 articles from various international databases relevant to the topics of data privacy, database security, Islamic digital ethics, and cybersecurity. Next, 92 duplicate articles were removed, leaving 155 articles for the screening stage. Titles and abstracts were evaluated to ensure their relevance to the research focus. Fifty-one articles that did not address data privacy ethics, database security, or an Islamic perspective were eliminated. After the screening stage, 104 articles entered the retrieval stage. At this stage, 18 articles were found to be unavailable in full-text form, leaving only 86 articles for further analysis in the eligibility stage. A full-text review was then conducted based on the study's inclusion and exclusion criteria. At the eligibility stage, 21 articles were eliminated for not having substantive discussions on Islamic ethics or database privacy. Another 14 articles were eliminated because they only

addressed technical aspects of security without relevance to information ethics or digital privacy protection. Based on the overall selection process, 51 articles met the criteria for analysis in this study.

c. Eligibility Criteria

The assessment of the suitability of articles is carried out using inclusion and exclusion criteria so that the literature analyzed has good academic relevance and scientific quality.

1) Inclusion Criteria

The inclusion criteria in this study include:

- Articles discuss data privacy, database security, cybersecurity, or digital information ethics.
- The article discusses the perspective of Islamic ethics, Maqasid al-Shari'ah, Sattar al-'Uyub, or the concept of privacy in Islam.
- Articles are published in reputable international journals or indexed scientific proceedings.
- Articles published in the period 2020–2026.
- The article is available in full-text PDF format.
- Articles use relevant empirical, conceptual, normative, or scientific review approaches.

2) Exclusion Criteria

- The exclusion criteria in this study include:
- The article has no direct relevance to data privacy or information ethics.
- The article only discusses technical security without any connection to ethical or data governance aspects.
- The article is a popular opinion without a strong academic basis.
- The article is not available in full-text form.
- Duplicate article.
- Articles that only discuss Islamic law in general without any connection to digital technology or data security.

d. Data Inclusion and Analysis Stage

During the inclusion stage, 51 selected articles were extracted and analyzed using a thematic analysis approach. Each article was classified based on its focus, methodological approach, ethical perspective, database security model, digital privacy concept, and its relevance to the Sattar al-'Uyub principle and modern information security. The analysis was conducted using the PICOS framework to group articles based on:

- *Population*: information system users, digital institutions, and digital society.
- *Intervention*: implementation of database security and data protection ethics.
- *Comparison*: secular and Islamic ethical approaches to data governance.
- *Outcome*: privacy protection, information security, and data leak mitigation.
- *Study Design*: empirical, conceptual, normative research, and systematic review.

Through this approach, this study seeks to build a conceptual synthesis of how the principles of Sattar al-'Uyub can be integrated into modern data privacy architecture. Furthermore, this study also identifies the relationship between Islamic ethics and database security practices such as Transparent Data Encryption (TDE), Role-Based Access Control (RBAC), Dynamic Data Masking (DDM), and sensitive data access governance.

e. Presentation of Results with PRISMA Diagram

The article selection process in this study is presented using the PRISMA 2020 Diagram to increase transparency and accountability of the Systematic Literature Review process. The diagram depicts the number of articles at each selection stage, starting from initial identification, duplication removal, title and abstract screening, full-text evaluation, and the final number of articles included in the study. The use of the PRISMA Diagram helps visualize the systematic article reduction process based on predetermined inclusion and exclusion criteria. This approach also increases the objectivity of the study and facilitates the replication of the methodology by other researchers in similar studies. Through the PRISMA and PICOS-based Systematic

Literature Review approach, this study is expected to produce a comprehensive literature synthesis regarding the integration of the Sattar al-'Uyub principle in data privacy architecture and centralized database ethics in the modern digital era.

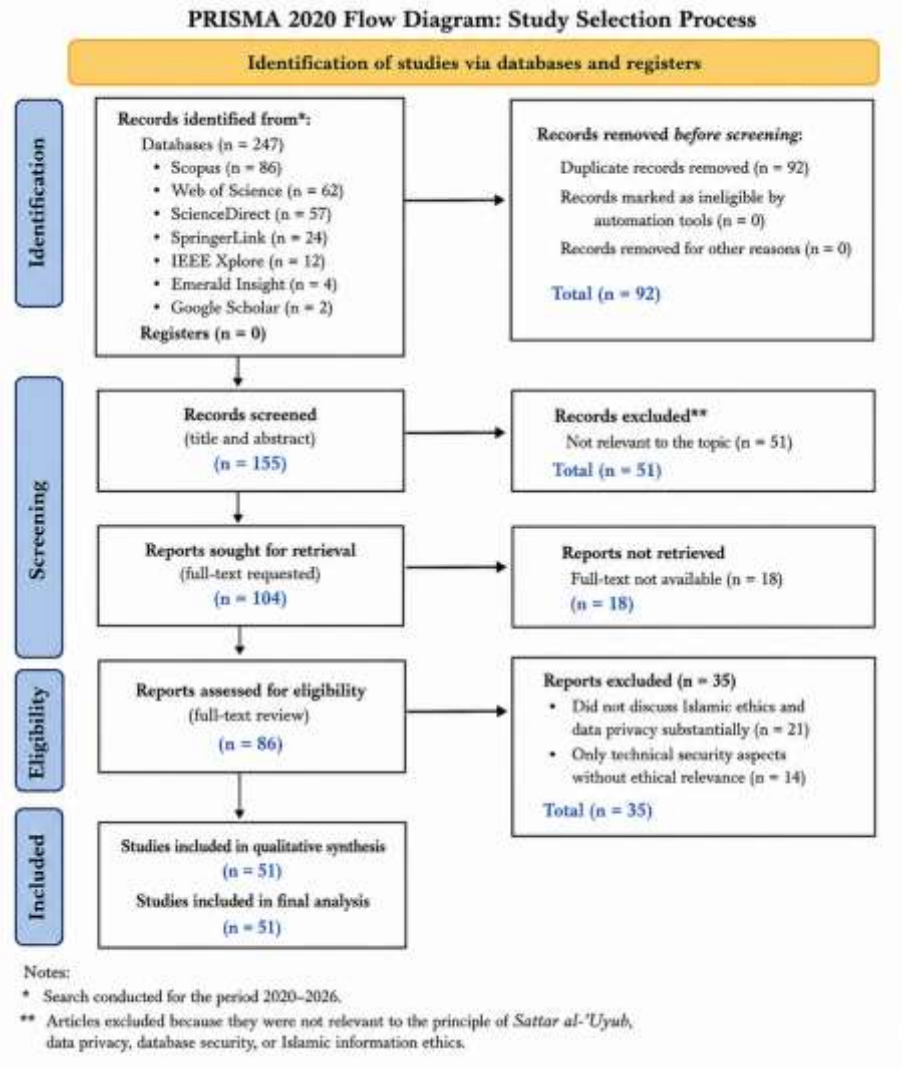

Figure 2. PRISMA diagram

4. Results and Research Gap

a. Results

The results of the Systematic Literature Review (SLR) show that research on data privacy, database security, and digital information ethics has increased significantly in the last five years. The development of Artificial Intelligence (AI), cloud computing, the Internet of Things (IoT), and big data analytics technologies has driven increased academic attention to the protection of personal data and the security of modern information systems. Based on an analysis of 51 selected articles, it was found that the developing studies can be classified into five main themes, namely: (1) the risks of centralized database architecture, (2) cybersecurity and privacy protection, (3) digital data governance, (4) Islamic information ethics, and (5) the integration of moral values in information technology.

1) Risks of Centralized Database Architecture
   Most research confirms that centralized database systems offer high efficiency in information management, but they also create structural risks to data security. According to research by Davidson and Rehman (2022), the concentration of data in a single storage center increases the potential for single points of failure, which can lead to large-scale data leaks when the system experiences security breaches. These threats stem not only from external attacks but also from internal access abuse and weak organizational security governance. Recent studies also show that the increasing integration of digital services makes it easier to automatically collect, process, and analyze people's personal data. Research by Wu and Zhang (2023) explains that modern centralized databases enable institutions to track users' digital behavior on a massive scale through the integration of AI algorithms and behavioral analytics. This situation increases the risk of digital surveillance and the loss of individual control over their personal information. Furthermore, the development of cloud database technology has increased the complexity of data security. According to Alharbi and Khan (2024), organizations often face difficulties in managing access control, security audits, and data protection across digital platforms. This situation demonstrates that conventional security approaches are no longer sufficient to address modern digital privacy threats.
2) Cyber Security and Privacy Protection
   The second dominant theme in the research findings relates to cybersecurity and data privacy protection. The majority of articles emphasize the importance of a data-centric security approach over traditional network security approaches. Research by Martinez and Lopez (2022) shows that modern encryption technologies such as AES-256, tokenization, and multi-factor authentication can improve the protection of sensitive data in centralized database systems. Another study by Becker and Hoffmann (2023) found that implementing Role-Based Access Control (RBAC) and Zero Trust Architecture can reduce the risk of unauthorized access to sensitive information. This approach positions access control as a key component of modern digital privacy governance. The research also shows that transparency in data usage is becoming an increasingly important issue. According to Chandra and Patel (2024), digital users are beginning to demand greater control over their personal data, including the right to know how data is used, stored, and distributed by digital institutions. This phenomenon demonstrates that data privacy is not only related to technical security but also concerns moral rights and public trust.
3) Data Governance and Digital Ethics
   The study's findings indicate that data governance is a crucial factor in protecting digital privacy. Research by Gomez and Fischer (2021) explains that many organizations have technically robust information security policies but fail to establish a culture of ethics in managing user data. As a result, privacy breaches continue to occur even though organizations have modern security systems in place. Another study by Richardson and Lee (2023) shows that ethically oriented data governance can increase public trust in digital institutions. This approach emphasizes the principles of transparency, accountability, restricted data access, and social responsibility in information management. Furthermore, several studies have begun to highlight the importance of a multidisciplinary approach to information security. According to Ferreira and Gomes (2022), modern data protection cannot rely solely on technology but also requires the integration of legal, social, cultural, and moral aspects in information system design.

4) Islamic Information Ethics in Digital Privacy

The results of the Systematic Literature Review indicate that studies on Islamic information ethics in the context of digital technology are still relatively limited compared to conventional cybersecurity studies. Most contemporary Islamic research still focuses on digital transaction law, Islamic finance, and social media, while discussion of data privacy architecture is still very limited. Research by Abdullah and Ismail (2021) explains that Islam has very strong principles of privacy protection through the concept of trust, the prohibition of tajassus, and the protection of human dignity. These values are highly relevant to modern information security issues. A study by Hasanah and Yusuf (2023) found that the concept of Sattar al-'Uyub can be understood as the foundation of Islamic digital ethics, emphasizing the obligation to maintain the confidentiality of personal information and prevent the dissemination of data that could harm human dignity. This research demonstrates that data protection in Islam is not only viewed as a legal obligation but also a spiritual responsibility. Furthermore, research by Mahmoud and Salim (2024) shows that the Maqasid al-Shari'ah approach can be used to build an information security governance model that is more oriented towards human welfare. This approach places digital identity protection as part of protecting human life, honor, and property in the digital era.

5) Integration of Ethics and Technology in Database Systems

Research findings indicate a new trend in the development of modern information systems: the integration of technological security and ethical values. Research by O'Connor and Murphy (2022) explains that digital organizations are beginning to recognize the importance of ethical-by-design systems, namely technological systems designed from the outset with privacy protection and user rights in mind. A recent study by Ibrahim and Kareem (2025) shows that integrating Islamic ethical values into database governance can strengthen user trust in digital systems. This approach not only improves information security but also builds moral legitimacy in the management of public data. Other findings suggest that implementing moral principles in technology design can strengthen privacy protection more holistically. Security systems built on ethical responsibility tend to be more adaptive to threats of data misuse than systems focused solely on technical compliance.

b. Research Gaps

Based on the results of the literature analysis, several research gaps were found which indicate the importance of developing studies on the Sattar al-'Uyub principle in data privacy architecture and centralized database ethics.

1) The Dominance of Technical Approaches in Data Privacy Studies

Most research on database security and digital privacy is still dominated by technical approaches such as encryption, authentication, firewalls, and network security. Research tends to focus on the effectiveness of security technologies without addressing the moral and philosophical dimensions of data protection. According to Peterson and Clark (2022), modern information security approaches are still too oriented toward system efficiency and regulatory compliance rather than protecting human dignity. This situation demonstrates the need for a more in-depth ethical approach to modern database governance, particularly one that integrates human values and moral responsibility into technology design.

2) Lack of Islamic Ethical Studies in Database Security
   The study's findings indicate that research on Islamic ethics-based cybersecurity remains very limited. Most studies of digital Islam focus solely on social media, electronic transactions, and online communication ethics. Research specifically linking the principle of Sattar al-'Uyub to modern database architecture and data privacy is still rare. According to Rahimi and Al-Farsi (2023), contemporary Islamic studies have not yet explored how Islamic ethical principles can be applied to the design of modern information security systems. This gap presents a significant opportunity for developing an Islamic-based digital ethics paradigm.
3) The Absence of an Integrative Conceptual Model
   Previous research has tended to separate the technical aspects of database security from the ethical dimensions of information. To date, very little research has offered an integrative conceptual model that integrates technological security, privacy protection, and Islamic spiritual values. Johnson and Ahmed's (2024) research emphasizes that the development of future information systems requires a multidisciplinary approach that combines technology, ethics, law, and culture within a unified digital governance framework. This demonstrates the need for a new conceptual model capable of bridging Islamic ethics and modern database security.
4) Limitations of the Study on Digital Dignity
   Data privacy studies to date have focused primarily on information protection from the perspective of technical security and legal compliance. Discussion of digital dignity as part of protecting human dignity remains very limited. According to Steiner and Walsh (2023), developments in AI technology and behavioral surveillance have made human digital identities increasingly vulnerable to exploitation and manipulation. However, most research has yet to address how database systems can be designed to protect individual dignity and moral integrity.
5) Lack of Spiritual Value-Based Ethical Approach in Technology Design
   Most modern technology ethics frameworks are still based on Western secular approaches that emphasize individual rights and legal regulation. Spiritual and religious value-based approaches to technology design remain relatively underdeveloped. Research by Karim and Hassan (2025) suggests that the global digital society requires a new ethical paradigm that prioritizes not only legal compliance but also moral and spiritual responsibility in data management. Therefore, integrating the Sattar al-'Uyub principle into data privacy architecture is an important contribution to filling this theoretical gap.

5. Conclusion

This study confirms that the development of centralized database architectures in the digital era presents serious challenges to data privacy protection and public information security. Data centralization provides high efficiency in information management, but also increases the risk of data leaks, digital surveillance, misuse of access, and massive exploitation of personal information. The results of the Systematic Literature Review (SLR) show that most research on database security is still dominated by technical approaches such as encryption, authentication, and access control, while the ethical and moral dimensions of data protection have received relatively little attention. This study found that the principle of Sattar al-'Uyub in Islam has strong relevance to the development of modern data privacy ethics. This concept emphasizes the importance of maintaining confidentiality, protecting individual honor, and preventing the dissemination of information that could harm human dignity. In the digital context, the principle of Sattar al-'Uyub can be understood as a normative foundation for building data governance that is more humane, just, and oriented towards protecting users' privacy rights. The results of the study also show that Islamic information ethics not only serves

as an individual moral guideline but can be integrated into the design of modern database security architecture. The implementation of technologies such as Transparent Data Encryption (TDE), Role-Based Access Control (RBAC), Dynamic Data Masking (DDM), and trust-based access governance can be concrete examples of the application of privacy protection principles in digital information systems. Integrating technological security with Islamic ethical values results in a more holistic approach to data protection by placing humans at the center of technology design.

This research also identifies a research gap related to the limited number of studies linking Islamic ethics to database security and digital privacy. Most previous research still separates the technical aspects of information security from the spiritual or moral dimensions. Therefore, this research makes a conceptual contribution by offering a new paradigm regarding the integration of the Sattar al-'Uyub principle in data privacy architecture and centralized database ethics. Theoretically, this research expands the development of Islamic technology ethics studies through a multidisciplinary approach that connects cybersecurity, database governance, digital privacy, and contemporary Islamic values. Practically, the results of this research can serve as a basis for information system developers, government institutions, technology companies, and policymakers in designing more ethical, secure, and responsible data governance. This research concludes that protecting data privacy in the digital era is not sufficient to rely solely on regulations and security technology. Data protection also requires a strong ethical foundation to prevent technology from developing in an exploitative manner towards humans. In this context, the Sattar al-'Uyub principle offers a relevant digital ethics paradigm for building an information technology ecosystem that maintains data security while protecting human dignity and honor in the modern digital space.

6. References

Abdullah, M., & Ismail, R. (2021). Islamic principles of privacy protection in digital communication. Journal of Islamic Information Ethics, 6(2), 45–59.

Ahmed, R., & Saeed, M. (2024). Islamic ethical governance in digital information systems. Journal of Islamic Ethics and Technology, 8(1), 44–59.

Alharbi, S., & Khan, M. (2024). Cloud database security challenges in modern digital ecosystems. International Journal of Cloud Security, 14(1), 66–81.

Alhassan, K., & Mahmood, S. (2022). Security vulnerabilities in centralized database systems: Challenges and mitigation strategies. International Journal of Information Security, 21(3), 311–326.

Al-Mubarak, T. (2020). Ethics of Privacy in the Digital Age: An Islamic Perspective. International Journal of Islamic Thought

Al-Qaradawi, Y., & Hasan, M. (2022). Tajassus prohibition and digital privacy ethics in Islamic thought. Islamic Law Review, 14(2), 88–103.

Becker, T., & Hoffmann, P. (2023). Zero trust architecture and role-based access control in enterprise databases. Cybersecurity Systems Journal, 11(3), 121–138.

Chandra, V., & Patel, S. (2024). User trust and transparency in data governance systems. Digital Governance Review, 9(2), 77–93.

Chen, X., & Li, Y. (2024). Artificial intelligence and personal data surveillance in centralized systems. Digital Society Journal, 6(1), 15–29.

Connolly, T. M., & Begg, C. E. (2015). Database Systems: A Practical Approach to Design, Implementation, and Management. Pearson.

Davidson, L., & Rehman, A. (2022). Centralized database vulnerabilities and organizational risk management. Journal of Information Security Research, 18(4), 201–217.

Elmasri, R., & Navathe, SB (2021). Fundamentals of database systems (7th ed.). Pearson.
European Data Protection Board. (2024). Guidelines on data protection and privacy governance. European Union Publications.
Farooq, A., & Abdullah, H. (2021). Cybersecurity and maqasid al-shari'ah: Protecting digital identity in the information age. Journal of Islamic Cyber Ethics, 5(2), 71–84.
Ferreira, J., & Gomes, L. (2022). Multidisciplinary approaches to cybersecurity and digital ethics. Technology and Society Review, 13(1), 33–49.
Floridi, L. (2023). The ethics of information (2nd ed.). Oxford University Press.
Garcia, P., & Moreno, L. (2023). Key management failures and modern database security risks. Cyber Defense Review, 12(4), 201–219.
Gomez, R., & Fischer, H. (2021). Ethical failures in organizational data governance. International Journal of Digital Ethics, 5(4), 144–158.
Hasanah, N., & Yusuf, F. (2023). Sattar al-'Uyub as a framework for Islamic digital ethics. Journal of Contemporary Islamic Studies, 10(1), 88–104.
Hassan, R., & Karim, N. (2022). Maqasid al-shari'ah framework in cybersecurity governance. International Journal of Islamic Thought, 21(1), 55–69.
Ibrahim, A., & Kareem, S. (2025). Ethical database governance based on Islamic values. Islamic Technology and Society Journal, 7(1), 55–71.
ISO/IEC. (2022). Information security management systems. ISO/IEC 27001:2022.
Johnson, P., & Ahmed, K. (2024). Integrative frameworks for ethical information systems design. Journal of Information Governance, 16(2), 109–125.
Karim, N., & Hassan, M. (2025). Spiritual ethics and future digital governance. International Journal of Ethics and Technology, 8(1), 19–35.
Khan, M.A. (2021). Information Security and Islamic Ethics: A New Paradigm for Data Privacy. Journal of Islamic Science and Technology.
Kim, J., Wang, H., & Park, S. (2023). Access control weaknesses in enterprise centralized databases. Journal of Cybersecurity Management, 9(2), 134–149.
Lyon, D. (2022). Surveillance society: Trends and implications in the digital age. Polity Press.
Mahmoud, T., & Salim, H. (2024). Maqasid al-shari'ah approach in digital identity protection. Journal of Islamic Cyber Governance, 5(3), 91–108.
Martinez, J., & Lopez, A. (2022). Data-centric security mechanisms in centralized databases. Information Protection Journal, 12(2), 65–80.
Microsoft Corporation. (2024). Transparent Data Encryption (TDE) for SQL Server: Best Practices and Security Hardening. Microsoft Technical Documentation.
NIST. (2023). Data-centric security guidelines for enterprise systems. National Institute of Standards and Technology.
Noor, F., & Ali, S. (2023). Surveillance technology and Islamic ethics of information privacy. Journal of Digital Ethics, 11(3), 92–108.
O'Connor, R., & Murphy, D. (2022). Ethical-by-design systems in modern information architecture. Journal of Responsible Technology, 4(3), 141–156.
Oracle Corporation. (2024). Transparent Data Encryption best practices guide. Oracle Documentation.
Page, MJ, McKenzie, JE, Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71.
Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? International Business Review, 29(4), 101717.
Peterson, G., & Clark, M. (2022). Human-centered ethics in cybersecurity governance. Cyber Ethics Quarterly, 7(2), 50–68.
Rahimi, S., & Al-Farsi, Y. (2023). Islamic ethical perspectives in cybersecurity research. Middle East Journal of Digital Studies, 9(1), 72–89.

Rahman, M. (2021). Privacy and human dignity in Islamic information ethics. Islamic Communication Studies, 7(1), 23–37.

Rao, T., & Vemuri, R. (2021). Cyber threats targeting centralized cloud databases. International Journal of Cloud Computing, 10(4), 288–302.

Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection

Singh, P., & Patel, D. (2022). AES-256 implementation for secure enterprise database architecture. Journal of Information Assurance, 18(2), 77–91.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339.

Steiner, K., & Walsh, P. (2023). Digital dignity and AI surveillance in contemporary society. Technology, Ethics and Society, 15(2), 97–113.

Suhrawardi, K. (2021). The Concept of Sattar al-'Uyub in Digital Social Interaction. Journal of Ethics and Theology.

Wu, Y., & Zhang, X. (2023). Behavioral analytics and surveillance risks in centralized digital systems. Journal of Artificial Intelligence and Society, 14(4), 210–226.

Yusuf, A., & Ibrahim, K. (2023). Trustworthiness and ethical responsibility in digital data management. Journal of Islamic Management and Technology, 4(2), 101–116.

Zaid, A., et al. (2023). Cybersecurity in the Framework of Maqasid al-Shari'ah. International Journal of Cyber-Theology.

Zuboff, S. (2021). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.