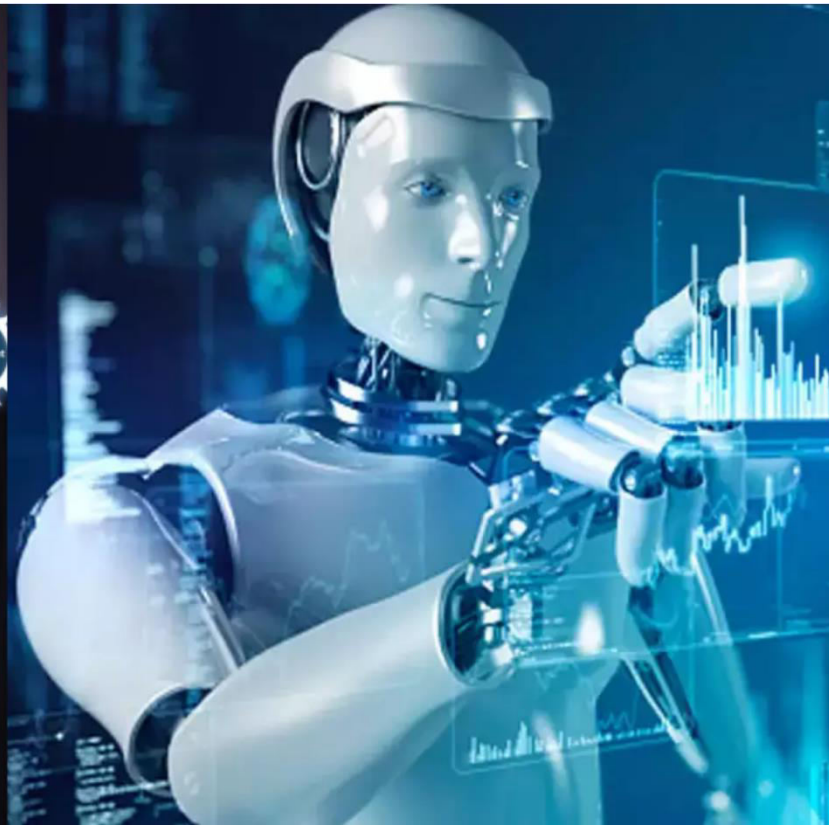
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405126|

Federated Dynamic Data Masking for IoT-Enabled Smart Energy Meters

Nischitha D N, Rakshitha U, Srinivas R, Vishwas Chandra M C, Promod Kumar B M

Department of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

Department of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

Department of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

Department of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

Assistant Professor, Department of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

ABSTRACT: With smart electric meters integrated into IoT, energy monitoring and billing revolutions will revolutioni ze. However, the continuous flow of sensitive consumer data reveals weaknesses in data protection. This article present s a complete softwarebased framework for Dynamic Data Masking (DDM) to maintain privacy without affecting the ac curacy of the solution. By using federated learning, the system identifies sensitive segments of a realtime measurement plant and masks them after monthly calculations. The architecture includes automatic PDF calculation generation with static masking of customer identity, dynamic masking of energy data, and mobile notification support. Simulations are done in Python, MySQL, and Riremlit to ensure cost-effective provisioning on a single laptop.

KEYWORDS: Dynamic Data Masking, Smart Meters, IoT, Privacy, Federated Learning, Energy Billing, Streamlit, MySQL, Data Security.

I. INTRODUCTION

Digital conversion of the power sector is revolutionised by intelligent IoT-enabled electric metering, as energy consumption is monitored, billed and managed. These systems offer great benefits, including real-time data collection, automated billing, remote access, and analytical control decisions. However, these benefits are related to urgent data protection offers. Intelligent counters collect fine-tuned energy consumption data from households, increasing risks and lifestyle behaviours that uncover personal consumption patterns. Traditional encryption methods protect data during transmission, but often do not protect data during peace, processing and analysis. This creates sensitive windows for unauthorized access or profile creation. To address these data protection concerns, we propose Federation Dynamic Data Masking (FDDDM) tailored to the smart electric female ecosystem. This solution introduces dynamic masking techniques based on spring-up learning to identify and protect sensitive data elements. This system is aggregated to use distributed local models to learn sensitivity patterns and build global masking models. It is important that dynamic masking is only used after monthly energy supply calculations. This will maintain operational efficiency while ensuring consumer privacy. This framework provides a practical, scalable, and software-related approach to data protection that provides intelligent measurement systems.

II. LITERATURE SURVEY

As IoT technology continues to integrate into critical infrastructures such as smart grids, ensuring privacy and protection of collected data is becoming increasingly important. The key mechanism used in this domain is data masking related to the process of hiding sensitive information, in order to protect user privacy and at the same time obtain the usefulness of the data for analysis. The literature on IoT security and intelligent measurements is strongly covered in encryption, authentication, and data access control. However, dynamic data masking remains a relatively unmistakable field, especially in conjunction with spring dyeing learning. However, these techniques often occur when data is stored and used for analysis. (2018) discusses a common technique for static masking where personal identifiable information (PII) such as names, e-miles, and addresses are replaced by symbolic values. This form of masking is typically used by data lakes and analytics platforms, anonymizing data records before running a query. It is effective for non-characteristic metadata, but is not suitable for real-time usage data such as energy consumption.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405126|

Energy consumption is constantly different and is stored for accurate billing. (2019) introduced differential data protection technology to mask aggregated energy consumption before reporting centralized servers. Various privacy is introduced randomly to maintain anonymity, which often affects the quality of actual insights and requires complex calibration to maintain the benefits. Dynamically adapting to custom masking guidelines, and using predictive modeling to identify confidential periods, also limits flexibility in actual billing systems. Study by Ahmed et al. (2020) proposed a politically managed engine for smart home devices that applies masking based on time and permission to access. The system effectively performed rule-based masking, but was not adaptable and learning abilities. Over time, it was not possible to adapt to developing user patterns or user behaviour. Furthermore, those solutions are not enhanced. This means that all decision-making and data aggregation have arisen potential data protection concerns for servers. Chatterjee et al. (2021) Dynamic masking system has been implemented in the IoT of healthcare systems. The system hidden sensitive tips like heart rate after diagnosis to comply with HIPAA regulations. This is conceptually similar to an intelligent meter system, where actual billing requires publicly available data, but allows long-term storage or reports to be anonymized. However, those approaches were based on static thresholds and manual rule configurations that were not automated and intelligence.

In contrast, Federated Learning is gaining attention as a data protection improvement technique, allowing for distributed model training without a portion of the raw data. Yang et al. (2022) applied federated learning to intelligent measurement devices to predict the best load requirements for some homes. Their model effectively learned consumer trends without affecting user data. However, their focus was not on sensitivity prediction or data masking, but only on load prediction. Existing solutions focus on masking identity fields or enforcing uniform guidelines that do not distinguish between critical and noncritical information. Furthermore, no significant task has been proposed to date to use dynamic masking after invoice calculations to maintain the accuracy of the billing and ensure that the data stored simultaneously is anonymized. First, static masking applies to strong customer datums such as names, e-mails, KEB numbers, addresses, and more. Second, after monthly electricity charges are generated, dynamic masking of timestamp measurements is performed. The most important innovation is in training local sensitivity prediction models for all smart meter nodes, recognizing patterns that undermine privacy (e.g., high consumption at unusual times). The final masking decision is made locally in this global model, ensuring privacy is preserved, but performance spending is kept to a minimum and accurate invoices are retained. This coalition approach is particularly well suited for resource-related environments such as rural India. In this environment, edge devices can participate in masking decisions without relying on centralized cloud processing. In contrast to other frameworks that use discriminatory privacy or encryption only, our solutions are practical and adaptive, focusing on the challenges of data modification, especially for smart meter infrastructure.

III. METHODOLOGIES

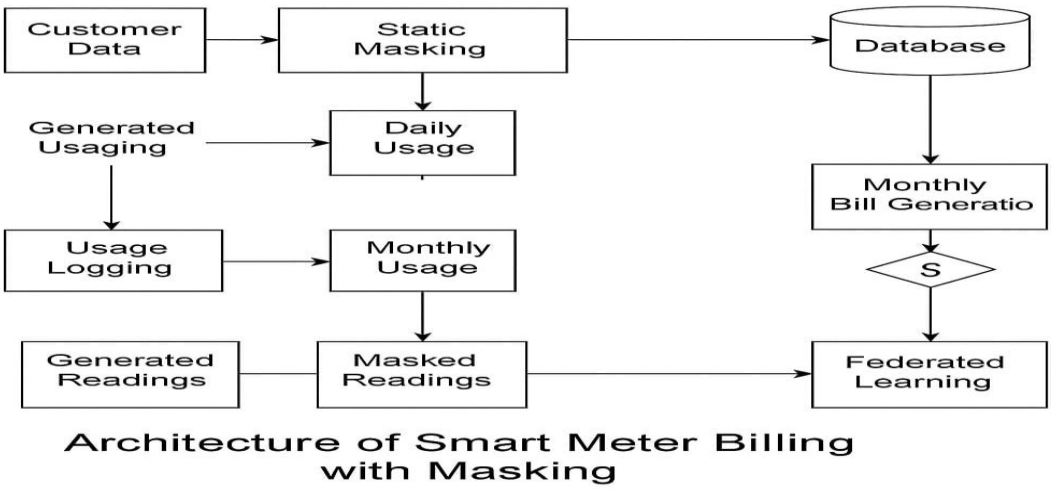


Figure 1

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405126|

Figure 1 shows the complete architecture of an intelligent measurement device integrated into static and dynamic data masking techniques. The framework starts with the generation of synthetic customer data, including personally identifia ble information (PII), such as name, email, address, and KEB account number. These fields are subjected to static mask ing to protect their identity. It is logged daily in parallel and stored as a timestamp in a MySQL database. After collectin g sufficient data, the system calculates monthly energy consumption and automatically generates invoices. As soon as t he billing is completed, dynamic masking will be applied to the sensitive portion of usage data before final memory. Th e database supplies masked costs with a light-
based user interface, allowing for safe visualization and customer interaction.

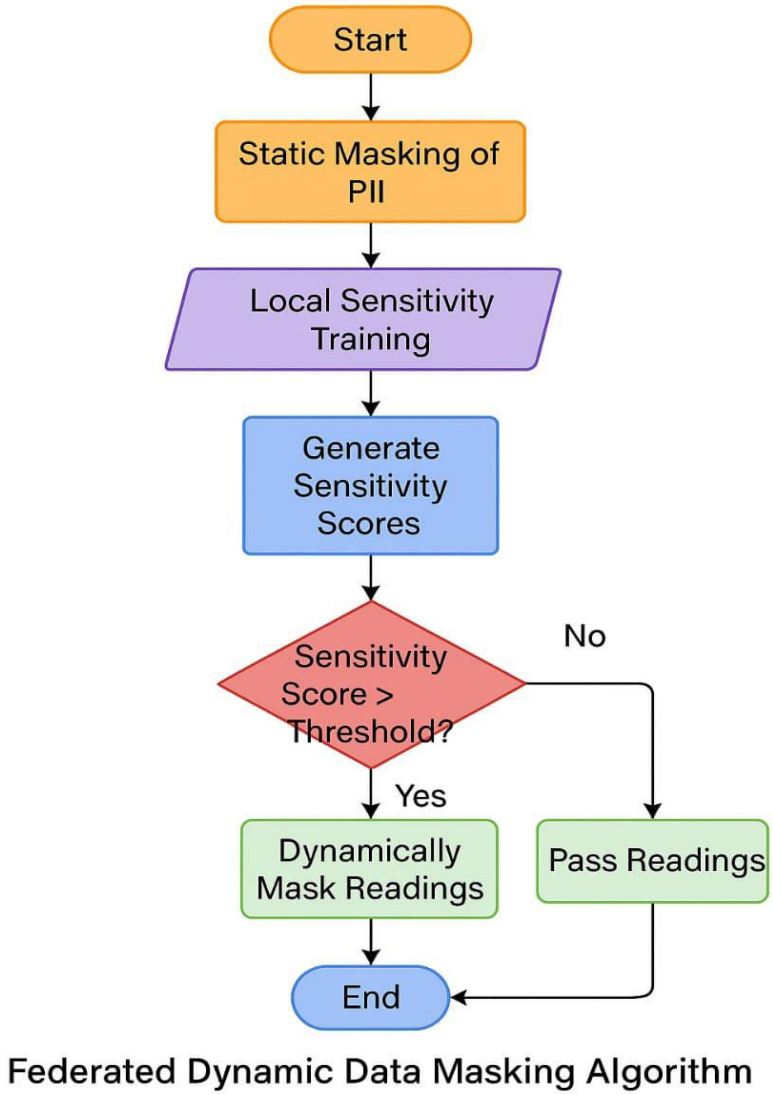


Figure 2

Figure 2 shows the federated dynamic data masking (FDDM) algorithm, a step-by-step flow that begins with static masking of PII. Each smart measurement device performs local sensitivity training based on usage behaviour to identify potentially sensitive data areas. These models calculate sensitivity values and compare them with predefined thresholds. Data points that exceed the threshold are masked, but the rest are still there. This ensures that only the compromise segment of data protection is veiled and that the rest is available for analysis or monitoring.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405126|

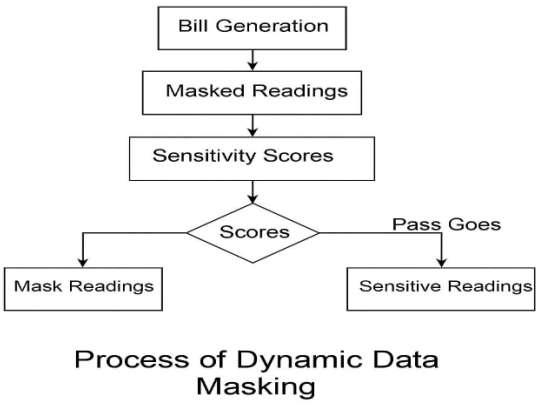


Figure 3

Figure 3 focuses on the process of dynamic data masking after billing. After calculating the energy costs, the system evaluates each measurement with a model for combined sensitivity prediction. Depending on the score, measurements are either unchanged or masked if they are classified as sensitive. This targeted masking approach ensures that actual consumption is affected, but long-term data storage meets data protection standards. The decision loop is clearly visualized and shows how sensitive it is. Sensitive data is not handled dynamically.

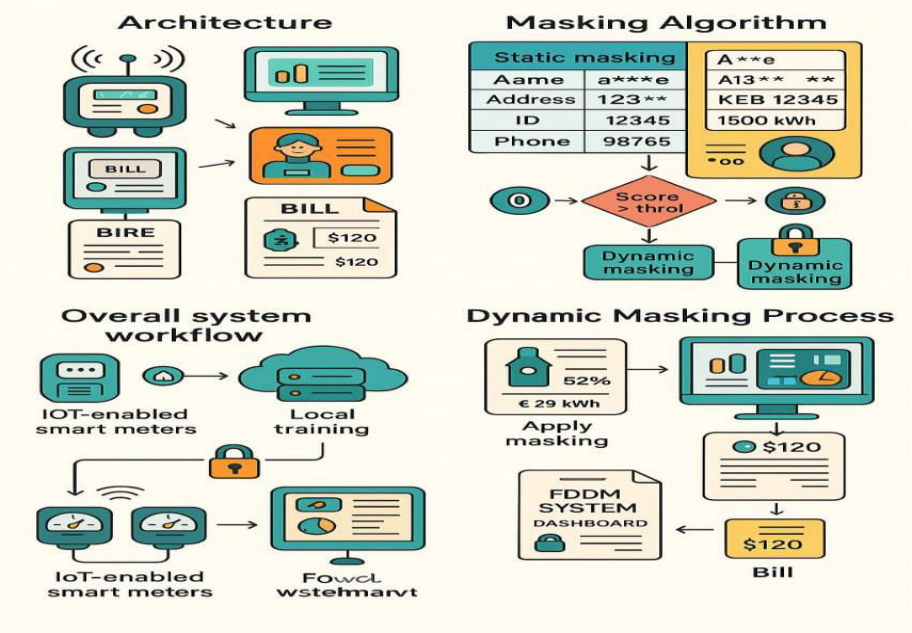


Figure 4

Figure 4 shows the overall tasks of the FDDM system. Here, the data collected by the smart knife is first sent to the central server, running a federation model and calculating the sensitivity values. Based on these reviews, measured values are selectively masked and transferred to the system dashboard, showing only the required and approved information. This process protects your resting consumer data while ensuring a seamless supply process, such as billing and reporting.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405126|

IV. RESULTS

Table: Actual Input and Expected Output for FDDM Project

Step	Input Data	Description	Actual Output	Expected Output
1	Customer dataset (Name, ID, Email, Phone, Address, KEB Account Number)	The input dataset with unique customer details	Data stored in local SQL database (SQL Table: random_customer_data)	Dataset stored with static masking (except phone and ID)
2	Meter readings (Timestamped kWh readings)	Meter readings captured per customer at specific time intervals	Raw meter readings recorded for each customer	Raw readings in database with customer-specific timestamps
3	Static Masking for Customer Data	Apply static masking to fields such as Name, Address, Email, and KEB Account Number (Phone and ID remain unmasked)	Customer data stored with static masking	Data masked (Name, Address, Email, KEB Account) except Phone and ID
4	Bill generation logic (Tariff, Tax Calculation)	Monthly electricity usage based on kilowatt-hour readings and tariff rates	Bills generated for each customer with proper calculation (e.g., Tariff, Tax, Total)	Monthly bill with breakdown (Usage, Tariff, Tax, Total)
5	Payment link generated	Use of customer's phone number to send payment link	Payment links sent via SMS to each customer	Payment links successfully sent to the customers' phones
6	Dynamic Masking on Meter Data	Apply dynamic masking to the meter readings (e.g., round or mask certain values) after bill generation	Masked meter data stored in the database	Meter data masked, ensuring privacy while maintaining billing accuracy
7	Federated Learning Model (Local and Global)	Local model training on customer data for dynamic masking decision	Local models trained per customer, Federated Averaging to generate global model	Global model trained using federated learning and applied to the data for dynamic masking
8	Streamlit UI Input (Frontend)	User interface for viewing statically masked data	Displays statically masked customer data (Name, Address, etc.)	Static data displayed correctly (masked fields, unmasked phone and ID)
9	Exporting to PDF	Generate PDF with bill details (including masking applied to data)	PDF with electricity bill generated for each customer	PDF generated with masked customer data and accurate bill
10	Customer Bill Notification	Notification with bill details and payment link	Customer receives notification with bill details and payment link	Customer receives the bill with accurate details and a payment link

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405126|

Details of Inputs and Expected Outputs:
Customer Data: This process starts with a data record containing basic customer details such as name, ID, email, phone, address, and KEB account number. This data is stored in a local SQL database. This data is subject to static masking on all fields except for phone number and customer-ID. The expected edition at this stage is that customer data is properly masked, personal information such as name, address, email, KEB account number is protected, and phone and ID are displayed for accurate claims. These measurements are stored in the database along with their respective timelines. The expected edition is that raw measurement data is correctly recorded for each customer. This ensures that Time Temple will be used over time. At this point, the entry is customer data and the static masking process applies to fields such as name, email, address, KEB account number, but the phone number and ID remain public. The expected edition is the proper storage of this masked data in the database to ensure that your personal data is protected. The expected performance is an invoice that includes a detailed breakdown of duties, taxes and overall use. Despite previous static masking, the accuracy of the law remains so that actual use will correctly charge customers. This includes the use of models for masking or rounding of specific data points to ensure privacy and at the same time maintain information essential for accurate billing. The expected output is that these masked measurements are stored in a database to protect customer data and at the same time maintain the core information needed for billing. This helps you train your global model to determine which parts of your data to mask. The expected edition is that data protection is ensured and a global model is generated to activate the exact billing process at the same time. The entry for this is statically masked data, and the expected edition is that the interface displays customer data with static masking applied to fields such as name, address, and phone numbers and IDs remain visible for proper identification and billing. The expected edition is creating a PDF for all customers with required billing details including masked customer data. This PDF serves as a safe way to present your customer's monthly electricity bill. This entry includes a final invoice and a payment link, and the expected issue is that the payment link is sent successfully to the customer via SMS or E-Mail, allowing you to pay the invoice safely.

V. CONCLUSION

With the proposed FDDDM framework, IoT -Smart Meate Netures customer data protection will be used in smart meter networks by using both static and dynamic masking, while maintaining billing integrity at the same time. Federation learning improves data protection decisions without data centralization. Laptop simulations prove that this approach is practical, scalable and could be used in practical applications. Future work will include real SMS API integration and expanding the environment using several devices.

REFERENCES

1. Y. Li, Z. Zhou, and X. Liu, “Privacy-preserving data analytics in smart grids: A review,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2805–2819, Apr. 2019.
2. R. Chatterjee, P. Mukherjee, and S. Bhunia, “Dynamic data masking in IoT healthcare environments,” *IEEE Sensors Letters*, vol. 5, no. 6, pp. 1–4, Jun. 2021.
3. M. Ahmed, H. Karim, and T. Bakker, “Context-aware privacy preservation in IoT-based smart homes using masking rules,” *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–26, Jun. 2021.
4. S. Shokri, R. Tronel, and J. Bos, “Federated learning for privacy-preserving smart metering,” in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2021, pp. 1–6.
5. L. Zhang, Q. Zhang, and K. Ren, “A privacy-preserving billing scheme for smart meters with load aggregation,” *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2084–2095, May 2020.
6. T. Nguyen, M. Roughan, and D. K. Sampath, “Data anonymization for the Internet of Things,” *Computer Communications*, vol. 174, pp. 30–45, Mar. 2021.
7. F. Yang, Q. Liu, T. Chen, and Y. Tong, “A survey on federated learning,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 6, pp. 2517–2536, Jun. 2022.
8. A. B. M. Al Islam and M. Chowdhury, “Privacy-aware dynamic masking for utility data,” in *Proc. IEEE International Conference on Computer and Communications (ICCC)*, 2022, pp. 1–6.
9. R. Agrawal and R. Srikant, “Privacy-preserving data mining,” in *Proc. ACM SIGMOD International Conference on Management of Data*, 2000, pp. 439–450.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details