KOMTEKINFO JOURNAL
LPPM Universitas Putra Indonesia YPTK Padang
Jl. Raya Lubuk Begalung, Padang, West Sumatera, Indonesia, Zip Code: 25221
Volume: 13, Issue: 2, Page: 83 - 88, June 30th, 2026, e-ISSN: 2502-8758
Available online at website: https://jkomtekinfo.org/ojs/index.php/komtekinfo

# Implementation of Isolation Forest for Anomaly Detection in Hospital Management Information System

Ibnu Putra[1]✉, Gunadi Widi Nurcahyo[2], Sarjon Defit[3]
[1,2,3] Master of Informatic Engineering, Faculty of Computer Science, Putra Indonesia University YPTK, Padang, 25221, Indonesia
bnuputra@gmail.com

**Abstract**

The digitization of the healthcare sector through the Hospital Management Information System (SIMRS) increases the risk of patient data security due to the potential for unauthorized access and misuse of sensitive information. The large volume of activity log data makes conventional sampling-based auditing processes ineffective in identifying security threats in real time. This study aims to implement user data access variables into the Isolation Forest algorithm framework to build an intelligent anomaly detection mechanism in the information system of Dr. M. Djamil Padang General Hospital. The research methodology applies an unsupervised machine learning-based Isolation Forest algorithm to isolate deviant behavior through anomaly scoring on random isolation trees. The pre-processing stage involves extracting request, status, and data size variables and performing numerical transformation using Z-Score standardization to maintain computational stability. The research dataset is sourced from the activity logs of the SIMRS web server at Dr. M. Djamil Padang General Hospital, with a total sample of 5000 user access transactions. The analysis results show that the model successfully identified 718 data points, or 14.36%, as anomalies with an accuracy rate identical to that of manual calculations. The application and implementation of the Isolation Forest technique proved to be effective in solving the problem of early detection of suspicious data traffic patterns in large data flows. The contribution of this research enhances hospital information security management through a data-based early warning system to improve the overall accountability of health information access.

Keywords: Isolation Forest, Anomaly Detection, Hospital Information System, Data Security



## 1. Introduction

Digitalization in the healthcare sector has driven the widespread adoption of information technology, covering various processes ranging from prevention, diagnosis, and therapy to continuous patient monitoring. One of the main manifestations of this digitalization is the implementation of the Hospital Management Information System (SIMRS), which serves as an integrated platform for managing clinical and administrative data across all service units. Although the existence of SIMRS significantly improves the speed, efficiency, and standardization of services, its widespread use has made issues related to data security and patient privacy increasingly crucial. This is due to increased potential risks, such as data leaks, unauthorized access, and misuse of sensitive information [1]-[3]. In addition, the high volume of user access log data makes manual auditing processes no longer adequate, requiring a rapid response mechanism to threats in the form of early detection and warning systems [4].

The urgency of strengthening data security is emphasized by various national policies, as stipulated in the Minister of Health Regulation on Electronic Medical Records [5], the development of the SATUSEHAT platform based on Fast Healthcare Interoperability Resources (FHIR) [6], and provisions in the Health Law [7], [8]. Various studies in Indonesia consistently show that although the implementation of Electronic Medical Records (EMR) and SIMRS provides many benefits to service quality, the challenges in maintaining the confidentiality, integrity, and availability (CIA) of health information are becoming increasingly apparent. Evaluation studies on the implementation of SIMRS highlight the need for comprehensive strengthening of governance, audit trails, and data security [9], [10]. Analysis in the context of hospitals and community health centers further emphasizes the importance of strict access control, reliable audit trails, and consistent security governance for risk mitigation [11], [12]. Furthermore, evaluations using the Human-Organization-Technology Fit (HOT-Fit) framework highlight that human, organizational, and technological factors must be aligned for SIMRS to function optimally and securely [13], [14].

Anomaly detection is the process of identifying patterns, events, or observations that deviate significantly from normal behavior in a dataset [15]–[17]. In the context of SIMRS, anomalies can appear as unusual access activities, use of modules beyond permitted permissions, or system interaction patterns

Submitted: 20-03-2026 | Revised: 16-04-2026 | Accepted: 23-05-2026 | Published: 30-06-2026

that do not correspond to clinical or administrative roles. The complexity of service processes, the diversity of work units, and the high volume of clinical and non-clinical transactions cause activity logs to grow rapidly, making manual auditing increasingly difficult [18]. This situation poses the risk of delayed detection of access abuse, procedural errors, or data governance violations. As a result, a systematic, scalable, and adaptive analytical approach is needed to strengthen operational security and hospital service quality.

In the context of SIMRS, anomalies can include unauthorized module access, shared account usage, or activity occurring at unusual hours [16]. The complexity of clinical and administrative processes, ranging from registration, outpatient services, pharmacy, support services, to insurance claims, generates extensive and heterogeneous activity logs. Sampling-based audits often fail to cover all variations, potentially causing early signals of access abuse to be missed [18]. Failure to detect these anomalies impacts service quality, compliance, and potentially leads to breaches of patient data security and privacy [19]. Therefore, a scalable, adaptive, and integrated analytical approach to the monitoring workflow is needed.

Dr. M. Djamil Padang General Hospital has a variety of roles, including doctors, nurses, pharmacists, analysts, cashiers, verifiers, and administrators, which create highly diverse access patterns. Fixed threshold rules (rule-based) are fragile because it is difficult to capture all variants of normal behavior across units and work shifts [20]. In addition, changes in policy, scheduling, and integration between modules cause shifts in normal patterns (concept drift), so that the baseline behavior quickly becomes obsolete. This condition requires a method that is able to learn from the majority of normal data while flagging unlabeled deviant events.

Dr. M. Djamil Padang General Hospital has a variety of roles, including doctors, nurses, pharmacists, analysts, cashiers, verifiers, and administrators, which create highly varied access patterns. Rule-based thresholds are inherently fragile because of the difficulty of capturing the entire spectrum of normal behavior variation across different units and work shifts [21]. In addition, policy changes, schedule adjustments, and inter-module integration cause shifts in normal patterns (concept drift), which quickly render behavior baselines obsolete. These conditions demand a method capable of learning from the majority of normal data while identifying deviant events without requiring predefined labels [15], [19], [20].

The Isolation Forest method generates anomaly scores by isolating observations through random trees in feature space [17], [20]. The characteristics of this algorithm enable efficient log processing and maintain label independence during routine operations. In addition, the scoring mechanism facilitates the setting of warning thresholds for daily operational use in hospitals [17], [25]. Isolation Forest isolates observations through random partitions, where observations that are isolated quickly and require fewer splits receive higher anomaly scores. Furthermore, this method offers several advantages: it is highly scalable, does not require labeled data, and remains robust to irrelevant features [17].

International studies have evaluated the performance of Isolation Forest through comparative analysis across various anomaly data domains in production environments [25]. In the field of network security, the Isolation Forest algorithm has proven effective in identifying unlabeled outliers, even in large-scale network traffic, making it a viable candidate for adaptation to user activity logs in health information systems [26]. These findings highlight the suitability of this method for analyzing user activity log data in the context of health information systems [25].

The ever-increasing volume of log data makes manual detection of deviant behavior in SIMRS user access logs increasingly difficult and inefficient. The need to comply with regulations related to Electronic Medical Records and data integration into the SATUSEHAT platform requires healthcare facilities to establish an early detection system for anomaly patterns in system logs [5]. The concept of unsupervised anomaly detection provides an ideal framework for identifying unusual patterns without requiring labeled data, making it highly suitable for application in hospital information systems [17], [24]. The Isolation Forest method translates this framework into operational anomaly scores, which can be used to trigger alerts and facilitate triage for further investigation [24].

The proposed solution is an Isolation Forest (IF) pipeline that processes activity logs periodically or in real time. The main stages include data cleaning, behavioral feature engineering, IF model training, and calculation of anomaly scores per session or activity sequence. These scores are then mapped to percentiles to set thresholds aligned with the triage capacity of the audit team. Each alert is accompanied by an activity trail summary, allowing auditors to immediately assess relevance and risk. This design maximizes the power of the IF algorithm as an outlier detector while minimizing unnecessary investigation overhead [27].

To be effective, the model must be integrated into a monitoring workflow that includes a warning priority dashboard, unit-specific notifications, and triage result logging. Auditor feedback is used to refine thresholds and update features, thereby improving the system's precision. Scheduled retraining is essential to mitigate concept drift, such as when service schedules, patient visit patterns, or module integrations change. Additionally, integration with internal compliance rules ensures IF signals remain aligned with access and security policies. A hybrid approach combining rule-based methods and Isolation Forest has been shown to

improve detection effectiveness while suppressing false positives [27].

Based on previous studies, this research proposes the implementation of the Isolation Forest method as a practical and strategic solution for detecting anomalies in SIMRS user activity in a hospital operational environment. The implementation of this design is expected to improve the efficiency of the security audit process and strengthen compliance with applicable policies in clinical service workflows.

This research aims to apply user data access variables in the Isolation Forest framework to detect anomalies in SIMRS at Dr. M. Djamil General Hospital. In addition, this research contributes by providing a foundation for improving information security governance on an organizational scale. This includes supporting datadriven decision making related to system security, refining user access policies, and improving overall system resilience.

## 2. Methods

Detection of anomalies in this study applies a quantitative approach with experimental methods to design and test a detection model. This study consists of several stages, starting from data collection, pre-processing, implementation model, detection anomalies, and evaluation result. The research framework is described in Figure 1 as follow.

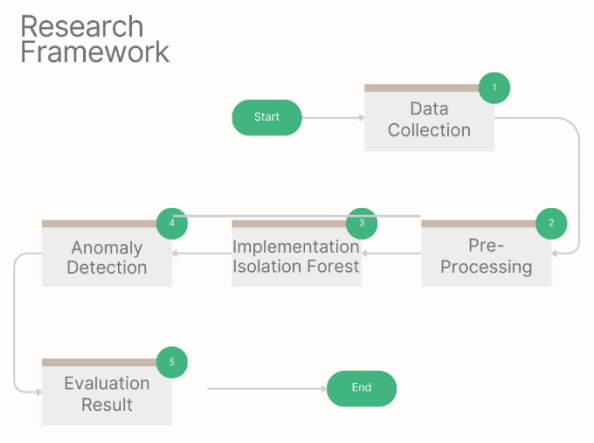


Figure 1. Research Framework

### *2.1 Dataset*

First stage is data collection, that was collected directly from the local server in the hospital's operational environment. This is different from public datasets, which are often simplified or cleaned up. The use of local log data aims to maintain the characteristics and complex behavior of actual users in the environment.

Data collection was performed in September 2025, and all incoming requests to the application server via the hospital's internal network were recorded. This ensured that the developed Isolation Forest model learned from data distribution patterns that truly represented the actual behavior of medical and administrative staff at the hospital. The total data collected for this study consisted of 2,541,678 rows, with 5,000 being allocated for model training. The sample of access logs are displayed in Figure 2 that would be analyzed.

```
172.16.99.31 - - [18/Sep/2025:15:23:23 +0700] "GET /backend/dist/webfonts/fa-
172.16.99.31 - - [18/Sep/2025:15:23:23 +0700] "GET /uploads/hospital_content/
172.16.99.31 - - [18/Sep/2025:15:23:23 +0700] "GET /backend/fullcalendar/dist/
172.16.99.31 - - [18/Sep/2025:15:23:23 +0700] "GET /backend/dist/webfonts/fa-
172.16.99.31 - - [18/Sep/2025:15:23:23 +0700] "GET /backend/signature/js/jque
172.16.99.62 - - [18/Sep/2025:15:23:23 +0700] "GET /screensaver/kodok.gif HTT
172.16.99.62 - - [18/Sep/2025:15:23:23 +0700] "GET /admin/daftarTilik/ceckDaf
172.16.99.63 - - [18/Sep/2025:15:23:23 +0700] "GET /admin/askep/getAskepMasal
```

Figure 2. Access Log

Figure 2 displays a sample of raw data from the server system that was used as the main dataset in this study. These logs capture user activity traces in real-time, including important attributes such as IP address (172.16.xx.xx), access time (timestamp), HTTP request method (GET/POST), response status code, and the size of data transferred. The analysis was conducted based on variables representing the characteristics of *log* and user behavior. Results of variable identification are used to be feature in the detection process. This is shown in Table 1 below:

Table 1. Feature to Use

| Variable | Log Attribute | Description |
|---|---|---|
| X1 | Request Method | String of the HTTP request. |
| X2 | Status | HTTP response code |
| X3 | Size | Response to client in byte |

Table 1 shows the simplification of log attributes into three main variables used as inputs (features) for the *Isolation Forest* algorithm. The variable X1 (*Request*) indicates the type of Hypertext Transfer Protocol (HTTP) request initiated by the user, which indirectly describes which module or service is accessed within the HIS. The variable X2 (*Status*) shows the response status from the server .The variable X3 (*Size*) is a measure of the response size, which frequently correlates with the complexity of the page or the volume of data transmitted. By directing the analysis toward these three variables, the model is able to identify the characteristics of the user access patterns both concisely and accurately, thereby making it easier to detect behavior that deviates from the normal patterns.

### *2.2 Pre-Processing*

In order to utilize access log data in a machine learning model, a series of preliminary steps must be undertaken. Firstly, the data must be thoroughly cleansed, involving the identification and removal of invalid data, duplicate logs, and missing values. Subsequently, parsing is performed on the log, particularly on the Request variable, to extract the URL and Request Method. Finally, the data must undergo transformation, wherein categorical or string variables in the Request are converted into a readable format. Attribute values

within the method category are converted into numerical codes based on predefined rules, where "GET" is assigned a value of 0 and "POST" is assigned a value of 1.

*2.3. Detection of Anomalies using Isolation Forest*

The implementation of the model started with the Random Partitioning stage, which is the process of randomly selecting features and split values between the minimum and maximum feature values to split the dataset.

This process is performed recursively until a Decision Tree (iTree) is formed, where the splitting ceases when the data is completely isolated or reaches a certain depth limit. The accumulation of these random trees then forms a Forest. Thereafter, a Path Length calculation is performed, which measures the number of steps required to reach the data point from the root of the tree.

The final stage of the process is anomaly determination (scoring) based on isolation logic. Data with a short *path length* is categorized as an anomaly due to its unique and easily separable nature. Conversely, data with a long *path length* is categorized as normal data due to its similar nature, which requires a more in-depth partitioning process. A score of anomaly s(x,n) is used to measure the level of strangeness of a sample x, defined as follows:

$$Anomaly\ Score = 2^{-\frac{E(h(x))}{c(n)}} \quad (1)$$

*2.4 Anomaly Detection*

Identifies anomalies in the data set using a model that determines whether the data is labelled as an anomaly (-1) or normal (1). The prediction based on the anomaly scores generated by the model, where samples with high scores are considered anomalies.

*2.5 Evaluation*

This stage of the process utilises qualitative validation and score distribution analysis. The most effective step is to perform Expert Validation (Top-N Check), which involves taking a sample of data with the highest anomaly scores and having these directly verified by domain experts to make sure that the anomalies found have relevant business or technical value.

## 3. Results and Discussions

In base of the explanation of the research framework, the objective of this study is to detect anomalies in server logs using Isolation Forest algorithm. The objective of Implementing the Isolation Forest model is to automate the data filtering process to identify rare events that are potentially dangerous or of high value. All of this can be done without having to train the model individually which events are normal and which are not, which is a significant advantage over traditional methods.

According to the data collection results, a total of 5,000 log data samples will be utilized in the present study. The pre-processing stage consists of the following procedure steps. Firstly, the method and URL are extracted and separated from the Request variable. Secondly, the attribute values in the method category are converted into numerical codes based on predetermined rules. The results can be seen in the Table 2 below.

Table 2. Transformation Data Result

| Ip | Request | Status | Size |
|---|---|---|---|
| 172.16.99.239 | 0 | 200 | 63 |
| 172.16.99.239 | 1 | 200 | 12969 |
| 172.16.99.73 | 1 | 200 | 1147 |
| 172.16.99.121 | 1 | 200 | 399 |
| 172.16.99.121 | 1 | 200 | 453 |

Based on Table 2 above, the attribute values within the method category are converted into numerical codes based on predefined rules, where "GET" is assigned a value of 0 and "POST" is assigned a value of 1.

This data will be processed by Isolation Forest algorithm, which operates on the principle of data isolation. The algorithm constructs a set of decision trees to measure how easily a data point can be separated from other data. The primary parameter produced by this process is the average path length. Log data with a short average path length will generate a high anomaly score. The result of implementation model show at Table 3 below.

Table 3. Anomaly Score

| Ip | Request | Status | Size | Anomaly Score |
|---|---|---|---|---|
| 172.16.99.239 | 0 | 200 | 63 | 0,152431761 |
| 172.16.99.239 | 1 | 200 | 12969 | -0,06279252 |
| 172.16.99.73 | 1 | 200 | 1147 | 0,055265985 |
| 172.16.99.121 | 1 | 200 | 399 | 0,029132614 |
| 172.16.99.121 | 1 | 200 | 453 | 0,016191203 |

The model successfully identified an anomaly in the second data set, with a size of 12,969. This was detected as an anomaly due to its value deviating significantly (outlier) from the mean of the other data sets, which were below 2,000 bytes. In the conceptual framework of Isolation Forest, the data points located in isolated regions of the data dimension space exhibit shorter path lengths. This results in negative scores and labels of -1.

The results of this model analysis are presented in Figure 3 below. Out of the 5,000 log entries analyzed, the model successfully classified 4,282 as normal activities and identified 718 as anomalies, representing a percentage of 14.36%.

📊 Isolation Forest Analysis Result:
Total Number of Data : 5000
Number of Normal Data : 4282
Number of Anomaly Data : 718
Percentage of Anomaly : 14.36%

🔎 5 Examples of Anomaly Data :

| | method | status | size | anomaly_score |
|---|---|---|---|---|
| 1 | POST | 200 | 12969 | -0.062793 |
| 7 | POST | 200 | 12969 | -0.062793 |
| 11 | GET | 307 | 31 | -0.207798 |
| 12 | GET | 307 | 31 | -0.207798 |
| 13 | GET | 307 | 31 | -0.207798 |

✅ 5 examples of Normal Data :

| | method | status | size | anomaly_score |
|---|---|---|---|---|
| 0 | GET | 200 | 63 | 0.152432 |
| 2 | POST | 200 | 1147 | 0.055266 |
| 3 | POST | 200 | 399 | 0.029133 |
| 4 | POST | 200 | 453 | 0.016191 |
| 5 | POST | 200 | 527 | 0.032069 |

Figure 2. Isolation Forest Analysis Result

The model evaluation process was conducted to assess the quality of the algorithm predictions utilised in the present study. This evaluation was qualitative and statistical in nature, wherein the implementation of the Isolation Forest model on 5,000 activity log samples generated statistical summaries and a list of Top-N Anomalies. A total of 718 anomalies were detected out of the 5,000 log entries. Preliminary analysis suggests that the anomaly rate of 14.36% is considered elevated for a stable system, where anomalies generally range from 1% to 5%. This finding indicates a high degree of sensitivity in the model threshold or the presence of highly diverse data traffic patterns (significant noise) within the hospital dataset. The distribution of anomaly scores generated by the Isolation Forest model across the dataset is displayed in Figure 3 below.

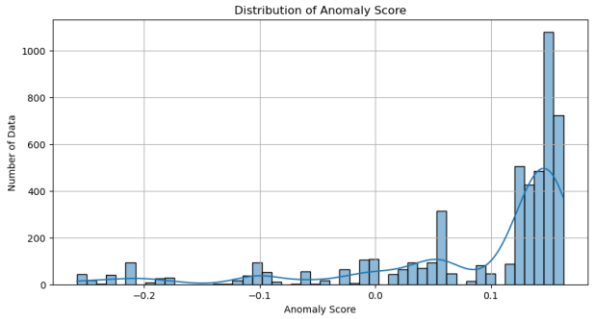


Figure 3. Distribution of Anomaly Score

## 4. Conclusions

Based on the research, implementation, and testing conducted regarding anomaly detection in Hospital Management Information Systems (SIMRS) using the Isolation Forest algorithm, it can be concluded that the objectives have been successfully achieved. Testing on 5,000 data samples revealed an anomaly detection rate of 14.36%, characterized by negative anomaly scores within the histogram distribution. An in-depth analysis of the Top-N Anomalies proved capable of significantly enhancing the precision of security investigations.This study provides a foundation for concrete access control recommendations, specifically the necessity of reviewing server routing configurations and implementing request size limits on firewalls to strengthen security compliance within the hospital environment.

Furthermore, this research contributes to help hospital information security governance through a data-driven early warning system, ultimately improving the overall accountability of health information access. Based on the limitations identified during the research process, several recommendations are proposed for future development and system enhancement. Identity Adding attributes such as IP Address or User Agent to improve detection context and better distinguish between human users and automated bots. Evaluating the performance of Isolation Forest against other anomaly detection algorithms, such as Local Outlier Factor (LOF) or Deep Learning approaches like Autoencoders and LSTM, to identify the most optimal model for hospital data characteristics. Implementing a feedback mechanism where IT administrators can label detection results as "True/False Positive." This feedback data can be utilized for model retraining to improve precision in recognizing emerging anomaly patterns.

## References


1] Suhariyono, U. S. (2025). Analisis Aspek Keamanan Informasi Data Pasien pada Penerapan RME. *Jurnal Manajemen Informasi Kesehatan Indonesia*. https://jmiki.aptirmik.or.id/jmiki/article/view/812

[2] Muchlis, C. R., & Sulistiadi, W. (2023). *Risiko Keamanan pada Implementasi SIMRS: Tinjauan Sistematis*. Jurnal Kesehatan Vokasional, 8(2), 89-97.

[3] Widodo, A. W., Hosizah, & Pertiwi, T. S. (2024). Persepsi Kemanfaatan & Kemudahan terhadap Perilaku Penggunaan SIMRS Berbasis Website di RSIA Kemang Medical Care Jakarta. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *12*(2). https://doi.org/10.33560/jmiki.v12i2.746

[4] Astuti, H. M., Sari, Y. A., & Arwan, A. (2023). Deteksi Anomali pada Log Aktivitas Sistem Informasi Akademik Menggunakan Isolation Forest. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *7*(10), 4684–4692. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/12975

[8] Kesuma, A. P. (2024). *Implikasi UU Kesehatan terhadap Tata Kelola Data Pasien*. Jurnal Hukum Kesehatan Indonesia, 15(2), 112–125.

[9] Saputra, C. H. (2024). Integrasi Audit Trail dan Teknik Clustering untuk Peningkatan Audit Keamanan Data. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*. https://jtiik.ub.ac.id/index.php/jtiik/article/view/8071

[10] L. Wujani dan A. Suardi, "Audit Trail pada Rekam Medis Elektronik," 2024.

[11] Wirajaya & Nugraha, "Evaluasi HOT-Fit Sistem Informasi," 2022.

[12] Saputra, C. H. (2024). Integrasi Audit Trail dan Teknik Clustering untuk Peningkatan Audit Keamanan Data. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*. https://jtiik.ub.ac.id/index.php/jtiik/article/view/8071

[13] Tabassum, M., Mahmood, S., Bukhari, A., Alshemaimri, B., Daud, A., & Khalique, F. (2024). Anomaly-based threat detection in smart health using machine learning. *BMC Medical Informatics and Decision Making*, 24, 347. https://doi.org/10.1186/s12911

[14] De Meulemeester, "Identifying Outliers in Medical Data," 2025.

[15] Ag Agyemang, K. O., Diaz, M., & Valero, M. (2024). *Large-Scale Unsupervised Anomaly Detection in Web Traffic*. Journal of Network and Computer Applications, 225, 103845.

[16] Lou, S. S., Liu, H., Warner, B. C., Harford, D. R., Lu, C., & Kannampallil, T. (2022). Predicting physician burnout using clinical activity logs: Model performance and lessons learned. *Journal of Biomedical Informatics*, 127, 104015. https://doi.org/10.1016/j.jbi.2022.104015

[17] Chua, T. H., Tan, S. C., & Lim, C. P. (2024). *Unsupervised Anomaly Detection for Data Streams: A Review*. Artificial Intelligence Review, 57(1), 1–45.

[18] Cao, Y., Zhang, H., & Li, J. (2024). *Feature-Resistant Isolation Forest for High-Dimensional Data*. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 1123–1132.

[19] Feng, W., Cao, Y., Chen, Y., Wang, Y., Hu, N., Jia, Y., & Gu, Z. (2025). Multi-granularity user anomalous behavior detection. *Applied Sciences*, 15(1), 128. https://doi.org/10.3390/app15010128

[20] Tabassum, M., Mahmood, S., Bukhari, A., Alshemaimri, B., Daud, A., & Khalique, F. (2024). Anomaly-based threat detection in smart health using machine learning. *BMC Medical Informatics and Decision Making*, 24, 347. https://doi.org/10.1186/s12911

[21] Chua, T. H., Tan, S. C., & Lim, C. P. (2024). *Unsupervised Anomaly Detection for Data Streams: A Review*. Artificial Intelligence Review, 57(1), 1–45.

[22] Hapsari, L. N., & Rokhman, N. (2024). Anomaly Detection of Hospital Claim Using Support Vector Regression. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *18*(1). https://doi.org/10.22146/ijccs.91857

[23] Saputra, C. H. (2024). Integrasi Audit Trail dan Teknik Clustering untuk Peningkatan Audit Keamanan Data. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*. https://jtiik.ub.ac.id/index.php/jtiik/article/view/8071

[24] Wijayanto, "Big Data Analytics in Healthcare," 2024.

[25] Feng, W., Cao, Y., Chen, Y., Wang, Y., Hu, N., Jia, Y., & Gu, Z. (2025). Multi-granularity user anomalous behavior detection. *Applied Sciences*, 15(1), 128. https://doi.org/10.3390/app15010128

[26] Binetti, M. S., Cauteruccio, F., & Terracina, G. (2024). A Comparative Evaluation of Isolation Forest in Production Environments. *IEEE Transactions on Knowledge and Data Engineering*, *36*(5), 2145–2158.

[27] Lubis, H. T., Roslina, & Tanti, L. (2025). Anomaly Detection in Computer Networks Using Isolation Forest in Data Mining. *Jurnal Teknik Informatika*, *18*(1), 77–86. https://doi.org/10.15408/jti.v18i1.44285

[28] A. Ramadhanu, H. Hendri, F. Hadi, D. Guswandi, D. M. Putra, R. Hardianto, and S. D. Rizki, "Hybrid decision support system and image processing for classifying priority applications in the Padang Government," CSRID (Computer Science Research and Its Development Journal), vol. 18, no. 1, pp. 178–191, 2026.

[29] A. Ramadhanu, H. Hendri, and F. Hadi, "Organic fertilizer content detection based on image segmentation and texture analysis," in Proc. 2025 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Dec. 2025, pp. 50–55.

## Biographies of Authors

**Ibnu Putra, S.Kom**