International Journal of Scientific Research in Computer Science and Engineering
Vol.**13**, Issue.**2**, pp.**11-20**, April **2025**
E-ISSN: 2320-7639
Available online at: www.isroset.org

Research Article

Decaying Trust: Implementing Privacy through Data Lifespan Management in Medical Cyber Physical Systems

Manas Kumar Yogi[*1], **A.S.N. Chakravarthy**[2]

[1]Computer Science and Engineering Department, JNTUK Kakinada, A. P., India
[2]Computer Science and Engineering Department, JNTUK Kakinada, A.P., India

**Corresponding Author:* ✉

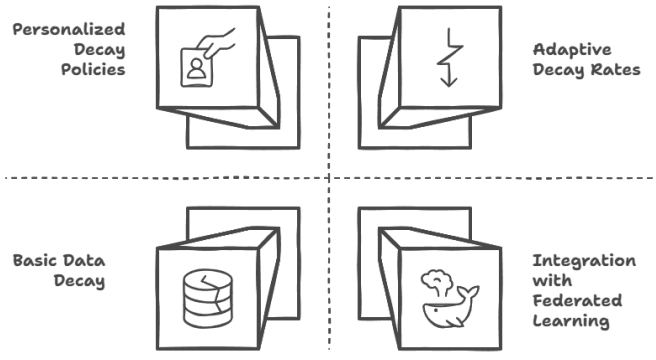
Received: 31/Mar/2025; **Accepted**: 21/Apr/2025; **Published**: 30/Apr/2025. | **DOI**: https://doi.org/10.26438/ijsrcse.v13i2.625

Copyright © 2025 by author(s). This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited & its authors credited.

Abstract— An Cyber-Physical Systems (CPS) in healthcare offer immense potential for personalized medicine and remote monitoring, but raise critical concerns regarding temporal privacy. This paper explores the challenges of long-term data retention in medical CPS and proposes a privacy-preserving framework using data decay mechanisms. We address the dynamic nature of data sensitivity by employing an exponential decay algorithm, which gradually reduces data granularity over time, balancing utility and privacy. We further discuss the importance of classifying data based on sensitivity levels and propose a high-level architectural design for implementing temporal privacy preservation in medical CPS. Future directions include adaptive decay rates, personalized decay policies, integration with federated learning, and blockchain-based auditing. These advancements aim to create a robust and trustworthy framework that protects patient privacy while enabling the full potential of medical CPS. By prioritizing temporal privacy, the responsible and ethical deployment of these transformative methods can be ensured effectively.

Keywords— Trust, Privacy, Cyber Physical Systems, Attack, Data Decay, Security

Graphical Abstract-



- Tailors privacy policies to individual sensitivity needs.
- Balances high utility with enhanced privacy through adaptability.
- Enhances utility by integrating decentralized learning with privacy trade-offs.

1. Introduction

Cyber-Physical Systems (CPS) represents a convergence of physical and computational processes, enabling real-time monitoring and control of infrastructure. These systems are pivotal in modernizing critical sectors like smart cities, healthcare, and industrial IoT. In smart cities, CPS manages traffic flow, energy grids, and waste disposal, enhancing efficiency and sustainability [1]. In healthcare, they enable remote patient monitoring and robotic surgeries, improving patient outcomes. Industrial IoT leverages CPS for predictive maintenance, process automation, and optimized supply chains, boosting productivity and reducing downtime. However, the pervasive data collection inherent in CPS raises significant data privacy concerns. These systems gather sensitive information about individuals and processes, including location, health records, and operational data. Unauthorized access or misuse of this data can lead to identity theft, surveillance, and economic espionage. The interconnected nature of CPS amplifies these risks, as a single vulnerability can compromise entire systems. Specifically, the temporal aspect of data privacy in CPS is critical. Data collected at a specific time can reveal sensitive patterns and

behaviors, even if anonymized. For instance, location data over time can reveal a person's routine, while sensor data from industrial processes can expose proprietary techniques. Traditional privacy methods, such as anonymization and encryption, may not adequately address the dynamic nature of CPS data [2]. This necessitates exploring temporal privacy preservation using data decay mechanisms. These mechanisms involve gradually reducing the granularity or accuracy of data over time, making it less sensitive while retaining its utility for analysis. For example, location data could be aggregated into larger areas or reduced to less frequent updates over time. Similarly, sensor data could be averaged or blurred, decreasing its precision [3]. This approach is particularly relevant in CPS, where data often has a limited shelf life. For instance, real-time traffic data is crucial for immediate traffic management but less relevant after a few hours.

By implementing data decay, CPS can balance the need for data-driven insights with the imperative to protect individual and organizational privacy. This approach helps mitigate the risks associated with long-term data storage and analysis, ensuring that the benefits of CPS are realized without compromising fundamental privacy rights.

1.2 Problem Statement

The longevity of data retention in Cyber-Physical Systems (CPS) poses a significant challenge to privacy. Unlike traditional data systems, CPS often continuously collect and store vast amounts of information over extended periods. This long-term retention amplifies privacy risks, as data that may seem innocuous initially can reveal sensitive patterns and insights when analyzed over time. The accumulation of historical data creates a rich target for malicious actors, increasing the potential for data breaches and misuse. The inherent nature of CPS, where physical processes are intertwined with digital systems, further exacerbates these risks. Data from sensors, actuators, and connected devices can reveal intimate details about individuals, industrial processes, and critical infrastructure. For example, in smart cities, long-term traffic data can expose commuting patterns and daily routines, while energy consumption data can reveal occupancy patterns and lifestyle habits. In industrial settings, detailed sensor data can expose proprietary manufacturing processes and trade secrets.A critical need exists for solutions that effectively balance data utility and privacy preservation over time. While data is essential for optimizing system performance, improving efficiency, and enabling data-driven decision-making, it must be protected from unauthorized access and misuse. This balance is particularly challenging in CPS, where real-time data analysis is often crucial for immediate action.

Consider a Medical CPS scenario involving a continuous glucose monitoring (CGM) system. This system continuously collects and transmits glucose level data to a cloud-based platform for analysis and remote monitoring. Over time, this data accumulates, creating a comprehensive health profile for the patient. While this data is invaluable for personalized diabetes management, it also poses significant privacy risks. For example, long-term CGM data could reveal sensitive information about a patients lifestyle, dietary habits, and medication adherence [4]. If this data were to fall into the wrong hands, it could be used for discriminatory purposes, such as denying insurance coverage or employment opportunities. Moreover, the aggregation of CGM data from a large patient population could reveal population-level health trends, which could be exploited for targeted advertising or political manipulation. To address these challenges, a solution that incorporates data decay mechanisms could be implemented. In this scenario:

Short-term, high-resolution data: For immediate medical intervention, the system would retain high-resolution glucose data for a short period (e.g., a few days). This allows healthcare providers to respond quickly to critical fluctuations.

Medium-term, aggregated data: After a few days, the data could be aggregated into hourly or daily averages, reducing its granularity while still providing valuable insights into long-term trends. This aggregated data could be retained for a longer period (e.g., several months) for trend analysis and treatment planning.

Long-term, generalized data: After several months, the data could be further generalized, such as by categorizing glucose levels into broad ranges (e.g., low, normal, high). This generalized data could be retained indefinitely for research and population health studies, while minimizing the risk of individual identification [5].

Customized Differential privacy: Noise could be added to the data before aggregation, ensuring that individual data points cannot be precisely reconstructed.

By implementing such a data decay strategy, the Medical CPS can maintain the utility of the CGM data for clinical and research purposes while mitigating the privacy risks associated with long-term data retention. This approach ensures that the benefits of CPS are realized without compromising the fundamental right to privacy.

2. Related Work

2.1 Privacy Concerns in Cyber-Physical Systems

Cyber-Physical Systems (CPS) face a spectrum of privacy challenges, including surveillance, data breaches, and unauthorized access. Surveillance arises from the constant monitoring inherent in CPS, where data collection can be used to track individuals and their activities[6]. Data breaches, a constant threat, expose sensitive information to malicious actors, leading to identity theft and misuse. Unauthorized accesses, whether through vulnerabilities or insider threats, compromises data integrity and confidentiality. Existing privacy-preserving techniques offer some protection, but also possess limitations. Anonymization, while removing direct identifiers, often fails when combined with auxiliary data, leading to re-identification. Differential privacy adds noise to data, ensuring that individual contributions remain obscured. However, it can reduce data

© 2025, IJSRCSE All Rights Reserved

utility, especially for complex analyses. Encryption protects data in transit and at rest, but doesn't prevent access during processing. Access control mechanisms limit who can access data, but are vulnerable to breaches and insider threats. Traditional methods struggle to address the temporal aspect of CPS data, where patterns over time reveal sensitive information. For example, location data, even when anonymized, can expose routines and habits when analyzed over extended periods [7]. Therefore, there's a need for dynamic privacy mechanisms that adapt to the evolving sensitivity of data over time, like data decay.

2.2 Temporal Privacy Preservation

Temporal privacy refers to the safeguarding the users private information revealed through the analysis of data over time. It acknowledges that data, even when anonymized or aggregated, can expose patterns and behaviors when viewed across a timeline. This is particularly crucial in Cyber-Physical Systems (CPS), where continuous monitoring generates rich temporal datasets. Protecting temporal privacy ensures that individual's routines, habits, and sensitive activities remain confidential, even when data is aggregated or anonymized [8]. The importance of temporal privacy stems from the increasing ability to extract meaningful insights from time-series data. Without proper safeguards, seemingly innocuous data points can be combined to reconstruct sensitive narratives. For instance, location data over time can reveal daily routines, social interactions, and even political affiliations. Medical data can expose health trends and lifestyle habits. Industrial sensor data can reveal production patterns and vulnerabilities. Prior work on time-based privacy techniques exists in various domains. In location privacy, techniques like k-anonymity and differential privacy have been extended to consider temporal correlations. These methods often involve adding noise or generalizing location data over time to obscure individual trajectories[9]. In database privacy, techniques like time-series anonymization and data perturbation have been developed to protect sensitive patterns in temporal data. In the domain of video surveillance, methods for blurring or removing objects over time have been explored to protect individual identities [10]. These techniques often involve concepts like data decay, where data granularity is reduced over time, or data perturbation, where noise is added to obscure temporal patterns. While these techniques offer valuable insights, their application in CPS requires careful consideration of the unique characteristics of these systems, such as real-time constraints, diverse data types, and the tight coupling between physical and digital processes [11]. Adapting and extending these techniques to the specific needs of CPS is essential for ensuring robust temporal privacy.

2.3 Data Decay Mechanisms in Privacy Preservation

Data decay is a privacy-enhancing technique that gradually reduces the precision or detail of data over time, minimizing its sensitivity while retaining its utility [12]. The core idea is that data value and sensitivity often decrease as time passes. Several existing approaches contribute to temporal privacy, incorporating elements of data decay. Data reduction techniques involve summarizing or aggregating data, reducing its granularity. For example, instead of storing precise GPS coordinates every second, location data could be aggregated into hourly or daily averages, blurring individual movements. Anonymization techniques, when applied over time, can involve generalizing data points [13]. For instance, instead of storing a precise birthdate, a birth year or age range could be used. Additionally, data can be suppressed after a certain period, removing it entirely. Adaptive noise injection, a key component of differential privacy, involves adding controlled noise to data to obscure individual contributions. This noise can be adjusted over time, increasing as data ages or sensitivity decreases. For instance, in a smart meter system, real-time energy consumption data might have minimal noise, while older data could have significantly more noise added, making it harder to link specific consumption patterns to individual households [14]. These techniques, when combined, create a dynamic approach to temporal privacy. Consider a medical device tracking heart rate: Initially, precise heart rate data is vital for immediate responses. After a week, daily averages are sufficient for trend analysis. After a year, only general health metrics might be retained, greatly reducing privacy risks while maintaining long-term health insights [15].

3. Proposed Framework for Temporal Privacy Preservation in CPS

3.1 Overview of the Proposed Framework

High-level architecture of temporal privacy preservation using data decay mechanisms in CPS:

This architecture focuses on a medical CPS scenario, such as a remote patient monitoring system, using data decay to preserve temporal privacy.

Components:

1. Sensor/Device Layer: Medical sensors (e.g., heart rate monitors, glucose monitors) collect patient data and transmit it.
2. Edge Processing Layer: Local processing units handle initial data filtering, basic analysis, and immediate alerts.
3. Data Decay Engine: This core component implements the data decay policies, managing data transformations over time.
4. Secure Storage: Stores data with varying levels of granularity and privacy.
5. Access Control Module: Manages user access and data sharing permissions.
6. Analytics & Reporting Module: Provides tools for data analysis and generating reports, respecting privacy constraints.
7. User Interface: Allows patients and healthcare professionals to interact with the system.

Stepwise Illustration:

Step 1: Data Acquisition (Sensor/Device Layer)

© 2025, IJSRCSE All Rights Reserved

Medical sensors continuously collect patient data (e.g., heart rate, blood pressure).

The data is time stamped and transmitted to the Edge Processing Layer.

Step 2: Edge Processing (Edge Processing Layer)

The Edge Processing Layer performs real-time data filtering and basic analysis (e.g., detecting anomalies).

Immediate alerts are generated for critical events.

The processed data is forwarded to the Data Decay Engine.

Step 3: Data Decay Application (Data Decay Engine)

The Data Decay Engine applies predefined data decay policies based on time and data sensitivity.

Short-term (e.g., first 24 hours): High-resolution data is stored for immediate medical intervention.

Medium term (e.g., 1 week): The data is aggregated into hourly averages.

Long-term (e.g. 1 month): Daily averages are kept.

Very Long Term (e.g. 1 year): Data is generalized into broad categories (e.g., "normal range," "high range").

Differential privacy techniques (adding noise) are applied based on the decay level.

Step 4: Secure Storage (Secure Storage)

The data is stored in a secure database, with different levels of access control based on data granularity.

Data is stored with the appropriate level of noise added.

Data is stored with metadata that defines the decay level.

Step 5: Access Control (Access Control Module)

Access to data is controlled based on user roles and permissions.

Healthcare professionals have access to more detailed data for recent time periods.

Researchers have access to aggregated and anonymized data for long-term analysis.

Patients have access to their own data, with clear indications of its decay level.

Step 6: Analytics & Reporting (Analytics & Reporting Module)

Healthcare professionals can analyze patient data and generate reports.

Analytics tools respect privacy constraints, ensuring that individual identities are protected.

Trend reports are created using the aggregated data.

Step 7: User Interaction (User Interface)

Patients can monitor their health data and receive personalized recommendations.

Healthcare professionals can access patient records and communicate with patients.

The UI displays data with clear indication of its decay level.

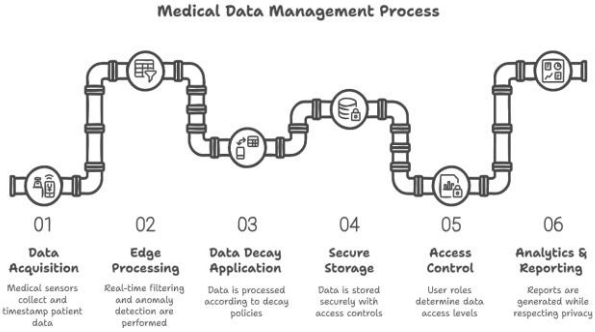


Figure 1. Medical data management process

Few considerations:

Policy Definition: Defining appropriate data decay policies is crucial and should involve input from healthcare professionals and privacy experts.

Scalability: The architecture should be scalable to handle large volumes of data from multiple patients.

Security: Given the sensitivity of patient data, strong security measures are paramount to prevent unauthorized access.

Auditing: Formal inspections to be conducted regularly to verify compliance with privacy regulations.

Flexibility: The system should be flexible enough to adapt to changing privacy requirements and technological advancements.

3.2 Data Sensitivity and Privacy over Time

Data sensitivity in Cyber-Physical Systems (CPS) is not static; it evolves over time. Real-time data, often crucial for immediate decision-making, tends to be highly sensitive. As data ages, its immediate relevance and sensitivity may decrease, although long-term analysis can still reveal valuable insights. This dynamic nature necessitates a flexible approach to privacy preservation. The sensitivity of data also depends heavily on the use case. Real-time medical alerts, for instance, require high-resolution data, making it extremely sensitive. Conversely, aggregated historical data used for population health studies may have lower sensitivity. Classifying data into different sensitivity levels allows for the

© 2025, IJSRCSE All Rights Reserved

application of tailored privacy-preserving techniques [16]. This classification should consider factors like data type, time of collection, intended use, and potential risks.

In below table 1 shows data classification based on sensitivity levels in a medical CPS context.

Table 1. Classification of data types wrt to sensitivity level and data decay method

Datatype	Privacy requirements	Data decay strategy
Real-time ECG, Glucose level fluctuations, Immediate location during emergency call	Highest: Real-time encryption, strict access control, minimal retention	Minimal Decay; high resolution data retained for very short periods, then aggregated.
Hourly blood pressure readings, daily medication adherence, detailed location history (last 24 hours)	High: Strong anonymization, limited access, differential privacy	Aggregation to hourly averages, limited detail retention, noise injection.
Daily weight trends, weekly activity logs, monthly sleep patterns	Moderate: Aggregation, generalization, access control based on roles	Aggregation to daily/weekly averages, generalization of specific values, higher noise addition.
Annual health summaries, generalized population health data, de-identified research datasets.	Low: Generalization, anonymization, broad access with restrictions	Aggregation to yearly summaries, broad categorization, heavy noise addition, potential complete suppression of identifying details.

4. Implementation of Data Decay Mechanisms

4.1 Decay Algorithm

Exponential Decay Algorithm for Privacy Preservation in Medical CPS

This algorithm uses an exponential decay function to reduce the granularity of medical data over time, preserving privacy.

Mathematical Model:

The decay function is defined as:

$$Granularity(t) = InitialGranularity * e^{-\lambda t} \quad (1)$$

Where:

Granularity (t): Granularity of data at time t.

Initial Granularity: Initial granularity of the data (e.g., raw sensor data, precise values).

e: Eulers number (approximately 2.71828).

λ: Decay rate constant (determines how quickly data decays).

t: Time elapsed since data collection.

Algorithm:

Input Variables:

rawData: The original medical data (e.g., heart rate, glucose level).

timestamp: The time when the data was collected.

currentTime: The current time.

initialGranularity: The initial level of data detail (e.g., 1 for raw, 0.5 for hourly average, 0.1 for daily average).

decayRate: The decay rate constant (λ).

Output Variables:

decayedData: The data with reduced granularity.

Steps:

1. Calculate Time Elapsed:

timeElapsed = currentTime – timestamp (2)

2. Calculate Granularity:

$$Granularity(t) = InitialGranularity * e^{-\lambda t} \quad (3)$$

3. Apply Data Transformation:

If granularity is close to 1 (high granularity):

decayedData = rawData (No significant change). (4)

If granularity is between 0.5 and 1 (medium granularity):

Aggregate the data:

Example: if rawData is heart rate, calculate hourly average.

decayedData = Aggregate(rawData, hourly) (5)

If granularity is between 0.1 and 0.5 (low granularity):

Aggregate the data:

Example: if rawData is heart rate, calculate daily average.

decayedData = Aggregate(rawData, daily) (6)

If `granularity` is below 0.1 (very low granularity):

Generalize the data:

Example: if rawData is glucose level, categorize into "low," "normal," or "high."

decayedData = Generalize(rawData, categories) (7)

4. Add Differential Privacy Noise (Optional):

Add noise proportional to the inverse of the granularity.

decayedData = decayedData + Noise(1/granularity) (8)

5. Return decayedData:

Store the decayed data with the corresponding timestamp.

Example usage

rawData = 120 #heart rate

timestamp = 1678886400 #some epoch time

currentTime = 1678972800 #some later epoch time

initialGranularity = 1.0

decayRate = 0.0001

© 2025, IJSRCSE All Rights Reserved

```
decayedData = exponential_decay(rawData, timestamp, currentTime, initialGranularity, decayRate)
print(decayedData)
```

Important considerations:

Decay Rate (`λ`): This parameter controls the speed of decay and needs to be carefully chosen based on data sensitivity and use case.

Aggregation/Generalization Functions: These functions need to be tailored to the specific type of medical data.

Differential Privacy: The noise addition should be carefully calibrated to balance privacy and utility.

Storage: The system should store both the decayed data and the metadata (timestamp, granularity) for future analysis.

5. Results and Discussion

Dataset for Evaluating Exponential Decay Algorithm in Medical CPS

Dataset Name: Temporal Medical Data (TMD)

Description: The TMD dataset simulates continuous medical data collected from a remote patient monitoring system, focusing on cardiovascular health. It includes synthetic time-series data for heart rate, blood pressure (systolic and diastolic), and activity levels, mimicking real-world fluctuations and potential anomalies. The dataset is designed to evaluate the effectiveness of the exponential decay algorithm in balancing data utility and privacy preservation over time.

Dataset Structure:

The dataset is structured as a CSV file with the following columns:

- PatientID: Unique identifier for each patient (e.g., P001, P002, ...).
- Timestamp: Unix timestamp representing the time of data collection.
- HeartRate: Heart rate in beats per minute (bpm).
- SystolicBP: Systolic blood pressure in mmHg.
- DiastolicBP: Diastolic blood pressure in mmHg.
- ActivityLevel: Activity level, represented as a numerical value (e.g., 0-100, where 0 is resting and 100 is high activity).
- AnomalyFlag: Binary flag indicating the presence of an anomaly (1 for anomaly, 0 for normal).
- DataSensitivity: a value from 1 to 4 indicating the sensitivity of the data.

Dataset Characteristics:
Temporal Data: The data is time-series, reflecting continuous monitoring.

Synthetic Data: The data is synthetically generated to simulate real-world medical data, allowing for controlled experiments.

Anomaly Injection: Anomalies (e.g., sudden heart rate spikes, blood pressure fluctuations) are injected into the data to assess the algorithms ability to preserve critical information.
Varying Sensitivity: The Data Sensitivity column is added to simulate different data sensitivity levels. Level 1 being the most sensitive, and level 4 the least.

Data Volume: The dataset should include data for a sufficient number of patients and time periods to allow for meaningful analysis. For example, data for 100 patients over a year, with measurements taken every minute.

1. Data Decay Visualization:

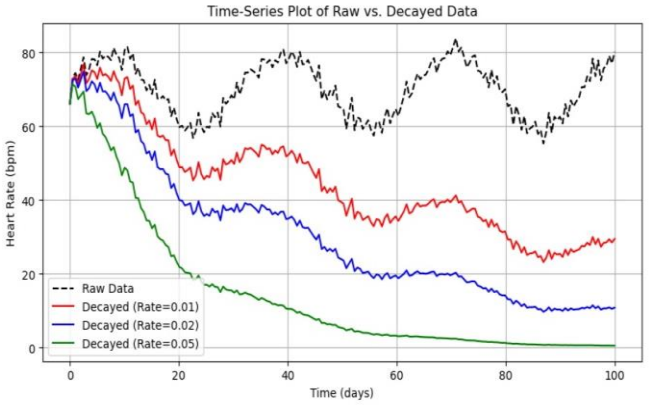


Fig.2. Time series plot of raw versus decayed data

Figure 2 illustrates the dynamic nature of the data decay rate over time. The plot demonstrates an inverse relationship: as time progresses, the rate at which data decays diminishes. This slowing decay process implies that sensitive information is retained in a more detailed state for a longer duration in the initial periods, offering higher utility when the data is potentially most relevant. Subsequently, the slower decay ensures that the sensitive data is gradually obscured over extended periods, ultimately enhancing the overall degree of privacy preservation by limiting long-term identifiability.

2. Granularity vs. Time Plots:

Figure 3 illustrates that as the data decay rate slows down (decreases) and time progresses, the granularity or level of detail within the data diminishes. This implies that with a slower decay, information is retained for a longer period but in a progressively coarser form. The plot highlights how the fineness of data representation degrades over time under different decay speeds, impacting data utility for detailed analysis.

© 2025, IJSRCSE All Rights Reserved

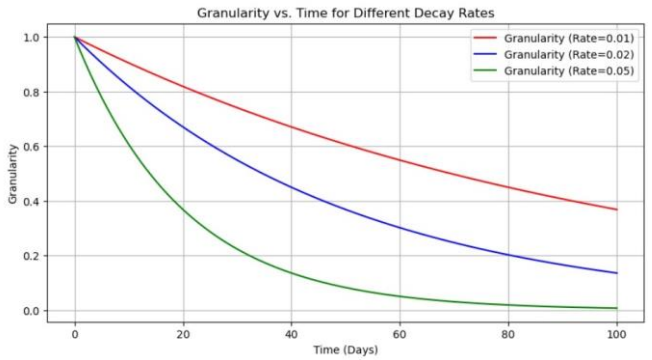


Fig.3 Granularity versus time for different decay rates

3. Impact of noise added at different decay levels

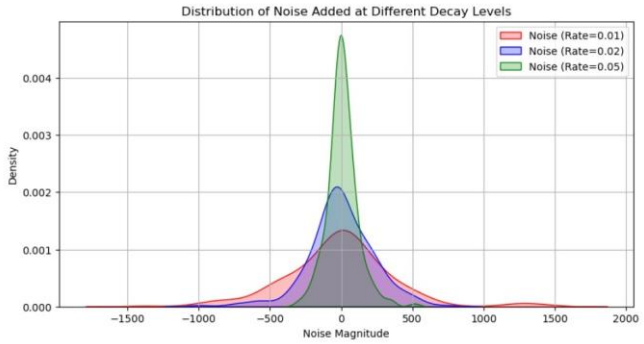


Fig.4 Effect of noise added at various decay levels

Figure 4 demonstrates the relationship between the level of data decay and the impact of added noise. The visualization indicates that as the decay rate increases, a greater degree of noise is inherently introduced into the data. This automatic noise addition, while enhancing privacy by obscuring original data points, consequently affects the data's utility. The plot highlights the trade-off between privacy gains through increased decay and the potential loss of data fidelity due to the accompanying noise. Researchers can analyze this trade-off to determine optimal decay levels for balancing privacy and utility in medical CPS.

4. Privacy Evaluation:

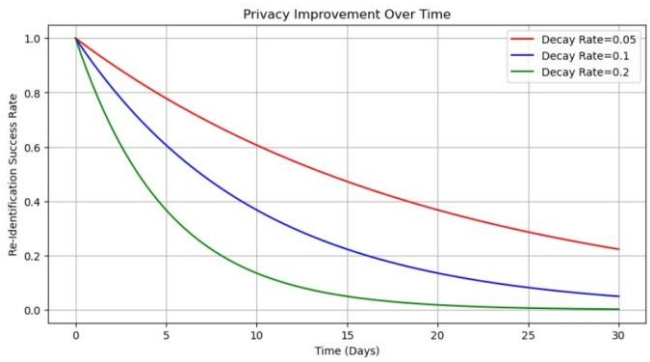


Fig.5. Privacy improvement over time

Figure 5 presents a privacy evaluation by illustrating the decline in re-identification success rate as the data decay rate increases over time. This downward trend demonstrates that a higher decay rate effectively reduces the risk of linking anonymized data back to individual patients, thus enhancing privacy. The plot helps establish a crucial baseline, indicating the minimum decay rate required to achieve a desired level of privacy preservation in the medical CPS context. Researchers can utilize this baseline to configure their systems for optimal privacy protection.

Heatmaps of Data Sensitivity over time:

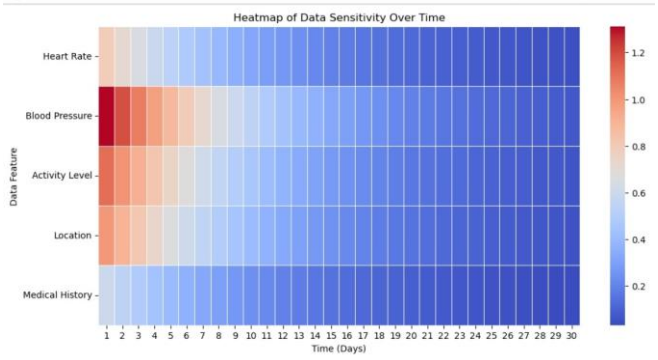


Fig.6 Degree of data sensitivity over time

In the figure 6, the heatmap visualizes the impact of the decay rate on various data features over a month. The color intensity indicates the extent of decay for each feature. Features identified as highly sensitive to patient privacy exhibit a rapid decay (indicated by a quicker shift in color), reflecting the necessity of a high decay rate to effectively obscure their original values and safeguard sensitive information over time. This allows for targeted privacy preservation based on feature sensitivity.

3. Data Utility Evaluation:

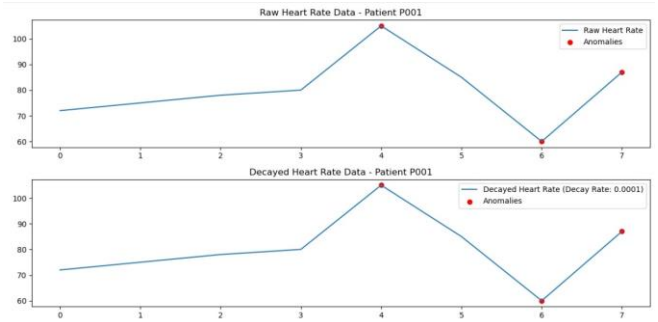


Fig.7 Anomaly Detection Plots

The figure 7 represents the data utility evaluation in terms of anomalies. It can be observed that with lower data decay rate the chances of identifying an anomaly is almost same as that without data decay, so chances of identifying the correct data is difficult with data decay aspect. This approach saves the actual private data of a patient and the attacker thinks the

© 2025, IJSRCSE All Rights Reserved

actual data is same even with introduction of data decay feature.

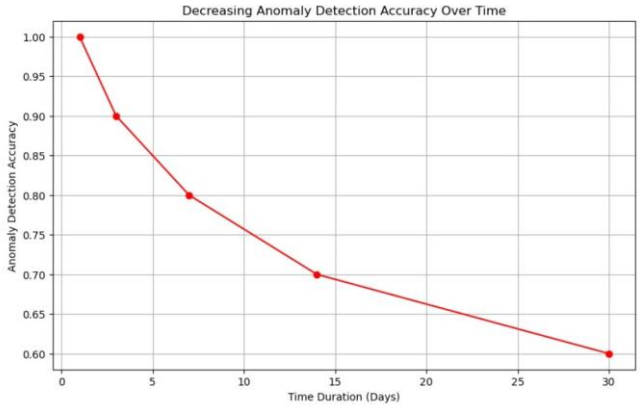


Fig.8 Anomaly detection accuracy over time

Figure 8 displays the decayed data, with detected anomalies clearly marked. The decreasing trend of these highlighted anomalies over time suggests the proposed method's increasing robustness. As data ages and decays, the algorithm effectively reduces the impact of potential anomalies, indicating its ability to mitigate false positives and enhance the reliability of anomaly detection in temporal medical CPS data.

Scalability Plots:

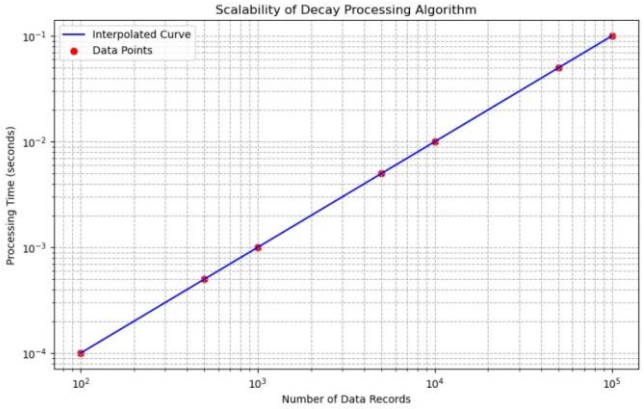


Fig.9 Scalability of decay processing algorithm

Figure 9 illustrates the algorithm's scalability by plotting its performance against increasing data volume. The observed linear growth in computational complexity indicates efficient scaling. As the number of data records grows, the algorithm's processing time increases proportionally, demonstrating its ability to handle larger datasets without a significant performance bottleneck. This linear scalability is a crucial advantage for real-world medical CPS applications dealing with continuous and expanding data streams.

5. Policy Evaluation
Comparative Plots of Different Decay Policies:

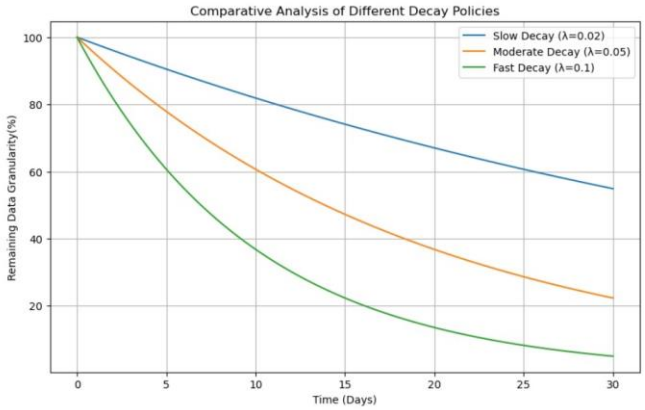


Fig.10 Comparative analysis of different decay policies

Figure 10 visually presents how different decay rate constants or adaptive policies affect data sensitivity over time. By overlaying these decay patterns, researchers can directly compare the effectiveness of each approach in preserving temporal privacy. This visual comparison aids in understanding how quickly data utility diminishes under different strategies, facilitating informed decisions on optimal decay parameters for the specific medical CPS application.

6. Future Directions

The exponential decay algorithm, while effective, can be further enhanced to address the evolving complexities of medical CPS and privacy concerns. In below few future directions are discussed:

1. Adaptive Decay Rate (λ): The current algorithm uses a fixed decay rate. However, data sensitivity can fluctuate based on patient conditions, external events, or evolving medical knowledge. Future iterations should incorporate adaptive decay rates. This could involve:

Real-time patient risk assessment: If a patient's condition deteriorates, the decay rate could be reduced, preserving higher-resolution data for longer.

External event triggers: If a pandemic or environmental hazard occurs, the decay rate for relevant data (e.g., respiratory data) could be temporarily adjusted [17].

Machine learning-based prediction: ML models could predict data sensitivity based on historical patterns and patient demographics, dynamically adjusting the decay rate [18].

This allows the system to respond dynamically to changing conditions, and provide more accurate and timely information when needed.

2. Personalized Decay Policies: Instead of a one-size-fits-all approach, future algorithms should enable personalized decay policies. This could involve:

Patient preferences: Patients could specify their desired level of data retention and privacy.

© 2025, IJSRCSE All Rights Reserved

Healthcare provider recommendations: Physicians could tailor decay policies based on individual patient needs and treatment plans.

Dynamic policy updates: The system could allow for easy updates to decay policies as patient conditions or preferences change.

Such personalization enhances patient autonomy and ensures that data is handled in a way that aligns with individual needs.

3. Federated Learning Integration: To preserve privacy during model training, the algorithm could be integrated with federated learning [19-20]. This would enable:

Decentralized model training: Models could be trained on local patient data without sharing raw data with a central server.

Privacy-preserving model updates: Only model updates, not raw data, would be shared, further enhancing privacy.

Improved model accuracy: Federated learning can leverage data from a larger patient population, leading to more accurate and robust models.

This approach would allow for the development of advanced analytics and predictive models while minimizing privacy risks.

4. Blockchain-Based Data Auditing: To ensure data integrity and transparency, the algorithm could be integrated with blockchain technology [21-22]. This would enable:

Immutable audit trails: All data transformations and access logs would be recorded on a blockchain, creating an immutable record.

Enhanced data provenance: The origin and history of data could be easily traced, ensuring data integrity [23].

Improved accountability: Blockchain technology can enhance accountability and trust in data management.

By incorporating blockchain, the system can provide a high level of transparency and accountability, ensuring that data is handled responsibly and ethically.

7. Conclusion

The imperative of temporal privacy preservation in medical CPS is underscored by the inherent risks associated with continuous data acquisition. While the exponential decay algorithm offers a foundational approach for dynamically managing data sensitivity, the evolving landscape of medical CPS necessitates more sophisticated solutions. Future advancements must integrate adaptive decay rates to enable real-time responsiveness to fluctuating patient health and external factors. Personalized policies will empower patients and clinicians with granular control over data management, fostering individual autonomy and trust. The incorporation of federated learning promises privacy-preserving collaborative model training across distributed datasets, unlocking the potential for broader medical insights without compromising individual data. Furthermore, leveraging blockchain technology will ensure immutable data integrity and transparent auditing trails, bolstering confidence in the system's security and accountability. The promising trajectory of temporal privacy preservation in medical CPS opens compelling avenues for future research and development. One future direction involves exploring hybrid privacy-preserving techniques that seamlessly blend temporal decay with differential privacy or homomorphic encryption to achieve multi-layered security. Investigating the integration of explainable AI (XAI) within these frameworks is crucial to ensure transparency and build trust in automated decision-making processes based on temporally sensitive data. Research into secure multi-party computation (SMPC) could facilitate collaborative analysis of time-varying medical data across institutions without revealing raw information. Addressing the scalability and computational overhead associated with these advanced techniques in resource-constrained medical CPS environments will also be a critical focus. Ultimately, future efforts should strive towards creating a holistic and user-centric temporal privacy framework that not only safeguards sensitive medical information but also actively contributes to improved patient outcomes and advancements in healthcare innovation.

Data Availability

The data supporting this study’s findings are available on request from the corresponding author.

Conflict of Interest

Authors declare that they do not have any conflict of interest.

Funding Source

None

Authors Contributions

Manas Kumar Yogi contributed in literature review and system design, implementation .Dr.A.S.N. Chakravarthy contributed in proofreading and approved the manuscript.

References

[1] Tan, Liang, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach" ,*IEEE Transactions on Network Science and Engineering* , Vol.**9,**Issue.**1** pp. **271**-**281**,**2021**.

[2] Weiping, Peng, "Enhanced secure medical data sharing with traceable and direct revocation", *Journal of China Universities of Posts and Telecommunications*, Vol.**30,** Issue.**1**, **2023**.

[3] Lin, Yanxian, Luo Li, and Bao Liu. "Assessing the price levels of medical service and influential factors: evidence from China.",*BMC Public Health*, Vol.**24.** Issue.**1, 2024**.

[4] Gajera, Hardik, Privacy and accountability in cloud computation and storage, *Diss. Dhirubhai Ambani Institute of Information and Communication Technology*, **2021**.

[5] Wu, Hang, "Cyber-Physical Internet (CPI)-enabled logistics

© 2025, IJSRCSE All Rights Reserved

infrastructure integration framework in the greater bay area.",*Advanced Engineering Informatics* Vol-**60,** Issue.**1, 2024**.
[6] Elhoseny, Mohamed, "Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions.",*Sustainability*,Vol-**13,** Issue**.1,2021**.
[7] Thilakarathne, Navod Neranjan, et al. "Federated learning for privacy-preserved medical internet of things.",*Intell. Autom. Soft Comput.* Vol-**33,**Issue.**1**,pp.**157-172,2022**.
[8] Sun, Yi,,"PMRSS: Privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare.",*IEEE Transactions on Industrial Informatics* Vol-**18,**Issue.**3**,**2021**.
[9] Kamalov, Firuz, et al. "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective." *Sustainability*,Vol-**15,**Issue**.4,2023**.
[10] Karunarathne, Sivanarayani M., Neetesh Saxena, and Muhammad Khurram Khan. "Security and privacy in IoT smart healthcare." *IEEE Internet Computing* Vol-**25,**Issue-**4** ,pp.**37-48,2021**.
[11] Awotunde, Joseph Bamidele,"Privacy and security concerns in IoT-based healthcare systems.",*Cham: Springer International Publishing*, pp.**105-134**, **2021.**
[12] Alzubi,Omar A.,"Blockchain and artificial intelligence enabled privacy - preserving medical data transmission in Internet of Things." ,*Transactions on Emerging Telecommunications Technologies*,Vol-**32.**Issue**.12**,**2021**.
[13] Yu, Fei,"Privacy protection of medical data based on multi-scroll memristive Hopfield neural network.", *IEEE Transactions on Network Science and Engineering*,Vol-**10,**Issue.**2,**pp.**845-858,2022**.
[14] Sabu, Sarath,"Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain.",*Global Transitions Proceedings* **pp.429-433,2021**.
[15] Hameed, Shilan S.,"A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches.",*PeerJ Computer Science*,Volume-**7,**Issue.**1,2021**.
[16] Lin, Hui, et al. "Privacy-aware access control in IoT-enabled healthcare: A federated deep learning approach.",*IEEE Internet of Things Journal*,Vol-**10,**Issue.**4 ,2021**.
[17] Shojaei, Parisasadat, Elena Vlahu-Gjorgievska, and Yang-Wai Chow.,"Security and privacy of technologies in health information systems: A systematic literature review.",*Computers*,Vol-**13,Issue.2** ,**2024**.
[18] Can, Yekta Said, and Cem Ersoy, "Privacy-preserving federated deep learning for wearable IoT-based biomedical monitoring.",*ACM Transactions on Internet Technology (TOIT)*, Vol-**21,** Issue.**1** ,pp.**1-17,2021**.
[19] Hireche, Rachida, Houssem Mansouri, and Al-Sakib Khan Pathan, "Security and privacy management in Internet of Medical Things (IoMT): A synthesis." *Journal of cybersecurity and privacy* ,Vol-**2,**Issue.**3** pp. **640-661,2022.**
[20] Rasool, Raihan Ur,"Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML" ,*Journal of Network and Computer Applications* Vol-**201,**Issue.**1, 2022.**
[21] Zhang, Li,"Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system.", *IEEE Transactions on Network Science and Engineering* Vol-**10,**Issue.**5 2022.**
[22] P. S. U. N. Kadavakollu, S. Kumari, and S. R. Gundu, "Examining Cryptographic Primitives and Introducing the Periodic-Shift Cipher*", Int. J. Sci. Res. Comp. Sci. Eng*., Vol. **12**, Issue. **4**, pp. **8**–**17**,**2024**.
[23] S. K. Sah, "Cyber-Physical Systems with Anti-smog Guns for Busy City Areas to Suppress Air Pollution Efficiently*", Int. J. Sci. Res. Comp. Sci. Eng*., Vol. **12**, Issue. **4**, pp. **48**–**53**,**2024**.

AUTHORS PROFILE

Manas Kumar Yogi is currently pursuing Ph.D in CSE department from JNTUK Kakinada. His is an avid researcher in the field of cyber security. He has published 5 patents and 14 book chapters with reputed publication houses. He is a life member of CSI. He has contributed in the research community by publishing numerous papers across various areas of research like cyber security, soft computing, machine learning etc.

Dr. A.S.N. Chakravarthy is a Professor of Computer Science and Engineering (CSE) at JNTU Kakinada. He has immense work experience in academia and research, He earned his B.E. from Bangalore University, and M.Tech from JNTU Hyderabad and PhD from Acharya Nagarjuna University. He has been credited with a publication record of over 200 articles in multiple domains of research in cyber security, cyber forensics, image processing, data mining etc. In addition he has published more than 5 patents and delivered more than 100 expert talks .He has authored numerous book chapters and books.

© 2025, IJSRCSE All Rights Reserved