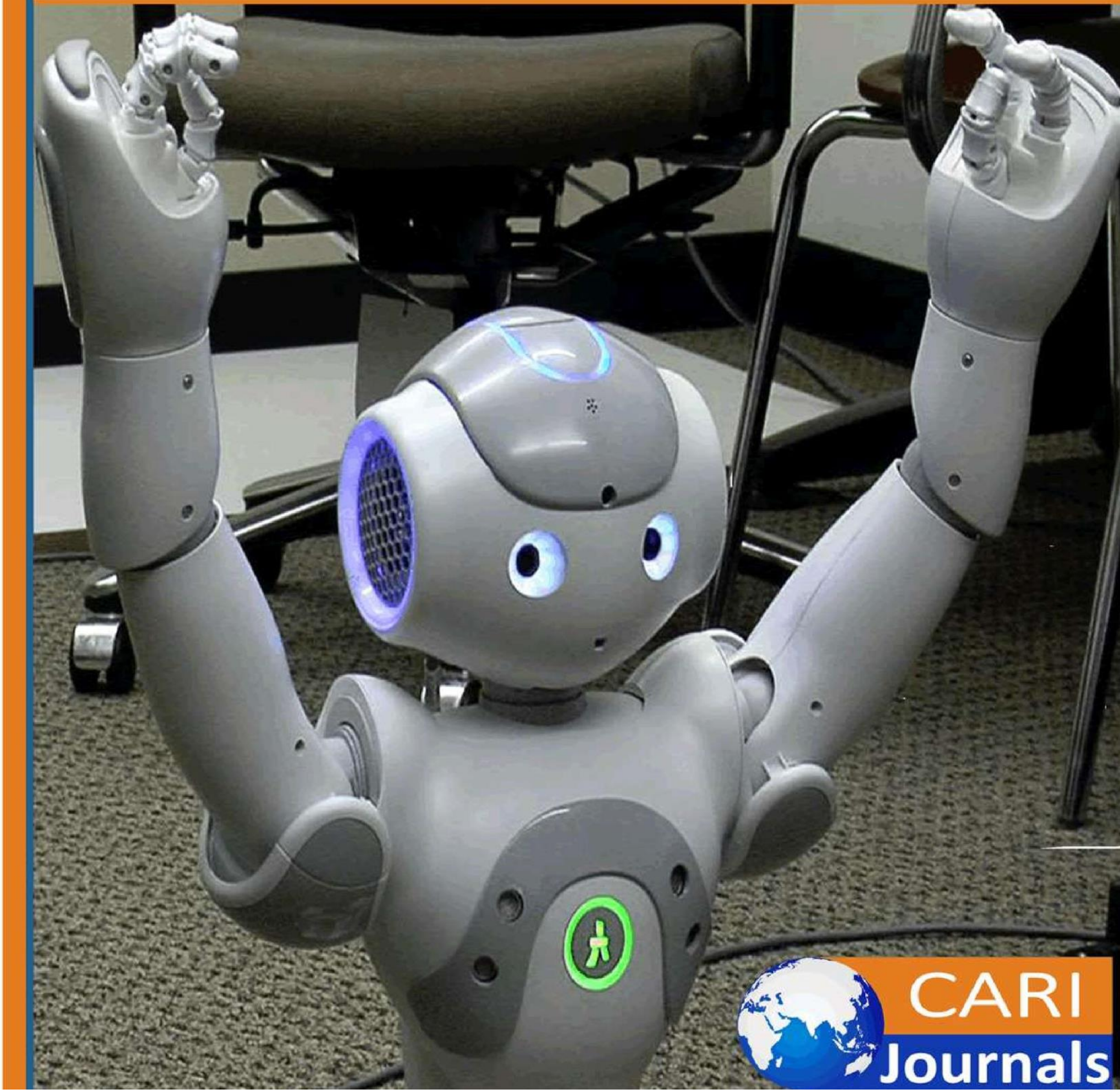
International Journal of
Computing and Engineering
(IJCE)

Securing Unified Data Models in Cyber Physical Systems: STRIDE–Based Approach



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 8, Issue No. 1, pp 1 - 12, 2026 www.carijournals.org

Securing Unified Data Models in Cyber Physical Systems: STRIDE–Based Approach

*[1]Eddie Musana, [2]Dr. Davis Matovu, [3]Dr. Richard Angole Okello, [4]Dr. Andrew Lukyamuzi
[1]PhD Candidate: Faculty of Engineering and Technology
https://orcid.org/0009-0002-0892-0146
[2]Senior Lecturer, Faculty of Engineering and Technology
[3,4]Senior Lecturer, Faculty of Science and Education
[1,2,3,4]Busitema University

Accepted: 4th Dec, 2025, Received in Revised Form: 25th Dec, 2025, Published: 5th Jan, 2026

Abstract

Purpose: This paper proposes a Secure Unified Data Model (UDM) Approach that enhances data security, trust, and reliability in Cyber-Physical Systems (CPS) by addressing data security risks such as breaches and unauthorized access.

Methodology: The methodology involved several steps. Reviewing existing literature to understand the current state of data modeling in Cyber-Physical Systems (CPS) and identify potential vulnerabilities. Supported by threat modeling and risk assessment frameworks, it analyzed data security risks for the Unified Data Model (UDM) in CPS. The focus was on protecting the UDM through strong encryption, access controls, security training, and regular assessments, safeguarding data at rest and in transit.

Findings: The findings show that a Secure Unified Data Model (UDM) approach improves data security in Cyber-Physical Systems (CPS) by strengthening access controls, encryption, and anomaly detection, thereby increasing CPS resilience against cyber threats. This promotes adoption in healthcare, smart cities, and governance. The secure UDM in CPS lowers breach risks, protects vendors and organizations, and offers scalable solutions that enhance productivity and reduce analytics costs. It supports safe data visualization, Business Intelligence (BI), and Artificial Intelligence (AI) tools, with potential applications in law enforcement for secure information sharing. The Secure UDM boosts trust, reliability, and compliance with data protection laws, encouraging adoption and innovation in critical sectors.

Unique Contribution to Theory, Practice and Policy: involves developing a conceptual Secure UDM framework that combines access controls, encryption, and anomaly detection for CPS. It also enhances understanding of UDM security in CPS contexts. Practically, this study provides actionable strategies for implementing secure UDMs across sectors such as healthcare, smart cities, and governance, thereby improving data security and trust in CPS through practical mitigation measures. Policy-wise, the study informs data protection regulations and standards for CPS and UDMs and encourages the adoption of secure UDM practices in critical sectors.

Keywords: *Cyber Physical Systems, Data Security, Unified Data Models*

1.0 Introduction

Unified Data Models (UDMs) are essential for improving security, trust, and privacy in CPS. They provide a standardized framework that enhances security through smooth data integration and fewer vulnerabilities, builds trust by ensuring consistent data handling and transparency, and protects privacy by centralizing data management and applying access controls. This ultimately increases CPS resilience against cyber threats across sectors like healthcare, smart cities, and governance (Busari & Bello, 2024). Cyber-Physical Systems (CPS) use UDMs to manage diverse data, but this integration introduces security risks like data breaches and unauthorized access. Protecting this data is crucial for CPS reliability. Unified Data Models in Cyber-Physical Systems combine physical and computational parts, enabling new applications across industries. Additionally, a Unified Data Model enables seamless data sharing and interoperability among components, laying the groundwork for efficient CPS operation.

Components of CPS that support the Unified Data Model include sensors, actuators, edge computing, and cloud computing. Sensors and actuators gather data from physical systems and perform actions based on processed data. Edge computing processes data closer to the source, reducing latency and enabling real-time decision-making. Cloud computing offers scalable infrastructure for data storage, processing, and analytics. Data Management Systems in CPS store, manage, and grant access to data through Unified Data Models. Communication Networks facilitate data exchange among components with standardized protocols. Intelligent Systems utilize Artificial Intelligence (AI), mimicking human intelligence, and Machine Learning (ML), allowing systems to learn from data, to analyze data. Sensors, actuators, edge computing, cloud computing, data management systems, and intelligent systems together support Unified Data Models. This integration allows for seamless data exchange, interoperability, and better decision-making in CPS. Data-driven methods improve performance and reliability in cyber-physical systems (Li et al., 2025)

Security data models include role-based access control (RBAC) for managing data access and an Access Control List (ACL), which is a list of permissions for resource access, supporting increased interconnectivity and large-scale data collection and sharing across organizations. (Nahla Davies, 2023) Emphasizes that a singular, interrelated network connected to a single source of truth enables organizations to achieve more efficient, accurate, and comprehensive performance analysis**.** As of 2019, companies were working with data from more than 400 sources (Nahla Davies, 2023)**.**

UDMs integrate data from Customer Relationship Management (CRM) systems, Enterprise Resource Planning (ERP) systems, and Business Intelligence (BI) tools. CRM manages customer information, ERP handles business processes such as finance, HR, and supply chain, while BI analyzes and visualizes data for decision-making. Offering a single access point creates a unified storage solution. With centralized data, business teams can implement security measures and leverage Artificial Intelligence (AI), which mimics human thinking, and Machine Learning (ML), enabling systems to improve automatically with data, as noted by (Nahla Davies, 2023). UDMs use integration identification to de-cluster data stored in different locations so that the consolidated data resides within a single Unified Data Model.

To create a unified data model, start by aligning it with your business goals, inventory all existing data sources, and outline your desired future state of data. Then, choose suitable platforms and integration technologies, emphasize data governance and security, and build a foundation for data quality, scalability, and user adoption. Man-in-the-Middle attacks made up 19% of all successful attacks on data in transit. This paper aims to advance technologies to secure data in transit and at rest for UDMs. The research gap in our study is the lack of data security risk analysis for Unified Data Models (UDMs) within the Cyber-Physical System working environment. It aims to develop a secure UDM, thereby enhancing knowledge and assessing the security of a UDM for end users of Cyber-Physical Systems (CPS).

Securing data in transit, which involves data moving across networks, is feasible through encryption that converts information into a code to prevent unauthorized access. This guarantees that data remains unreadable by unauthorized users during transmission. Data encryption protocols for transit data include Hyper Text Transfer Protocol Secure (HTTPS), which encrypts web-based communications; Transport Layer Security (TLS), which safeguards data exchanged over a network; and Secure File Transfer Protocol (SFTP), which securely transfers files. These protocols are essential for maintaining data integrity (accuracy and consistency) and confidentiality (preventing unauthorized access) during transmission (Alexandre Diard, 2025). This paper emphasizes the development of a secure UDM for CPS that securely meets end users' needs for data protection. A 2019 Market Pulse study found companies accessed data from over 400 sources. More than 20% of companies accessed data from over 1,000 sources. UDMs enable organizations and end users to synchronize and engage with data more effectively (Alexandre Diard, 2025).

According to the 2020 Experian report, although 85% of organizations recognize the value of data, most face challenges with effective data management (Zubin et al, 2025).

A February 2023 Financial Action Task Force (FATF) plenary report (Barigye, 2024) notes a rise in ransomware attacks. Targets include financial institutions, digital assets, and organizational data. Criminals often use Virtual Assets (VAs) to move large sums quietly. The report explains how cybercriminals launch ransomware, launder payments, and detect risk indicators. These indicators help organizations spot and prevent ransomware-related suspicious transactions. In Uganda, cybercrime is a critical issue. During the 2023/2024 financial year, 245 cases were reported, a 14.3% decrease from 286 in 2022. Despite this, financial losses exceeded **1.5 billion** UGX (**UGX 1,543,292,161**) in 2023, with only **UGX 377,441,465** recovered (Barigye, 2024).

Cybercrime often relies on data to execute attacks, highlighting the need for stronger encryption (methods for making data unreadable without authorized access) for data in transit (data being moved between devices) and at rest (data stored on systems). Enhanced data encryption further secures sensitive information against cyber threats and helps prevent data compromise, thus supporting a secure UDM. Security training (educational activities to increase staff awareness of cyber risks) strengthens an organization's resilience against attacks. It ensures protection for personal, organizational, financial, and digital data, whether at rest or in transit (Madnick, 2023). The significance of this paper is that securing Unified Data Models (UDMs) for Cyber-Physical Systems (CPS) is essential, as it safeguards sensitive information, ensures system reliability, and fosters trust, ultimately encouraging the adoption and innovation of trustworthy CPS.

2.0 Literature Review

Man-in-the-Middle attacks made up 19% of all successful attacks on data in transit. This paper aims to advance technologies to secure data in transit and at rest for UDMs.

The research gap in our study is the lack of data security risk analysis for Unified Data Models (UDMs) within the Cyber-Physical System working environment. It aims to develop a secure UDM, thereby enhancing knowledge and assessing the security for UDM end users in Cyber-Physical Systems (CPS).

Securing data in transit, which involves data moving across networks, is feasible through encryption, converting information into a code to prevent unauthorized access. This guarantees that data remains unreadable by unauthorized users during transmission. Data encryption protocols for transit data include Hyper Text Transfer Protocol Secure (HTTPS), which encrypts web-based communications; Transport Layer Security (TLS), which safeguards data exchanged over a network; and Secure File Transfer Protocol (SFTP), which securely transfers files. These protocols are essential for maintaining data integrity (accuracy and consistency) and confidentiality (preventing unauthorized access) during transmission (Alexandre Diard, 2025). This paper emphasizes the development of a secure UDM for CPS that securely meets end users' needs for data protection.

A 2019 Market Pulse study found companies accessed data from over 400 sources. More than 20% of companies accessed data from over 1,000 sources. UDMs enable organizations and end users to synchronize and engage with data more effectively (Alexandre Diard, 2025). According to the 2020 Experian report, although 85% of organizations recognize the value of data, most face challenges with effective data management (Zubin et al, 2025).

A February 2023 Financial Action Task Force (FATF) plenary report (Barigye, 2024) notes a rise in ransomware attacks. Targets include financial institutions, digital assets, and organizational data. Criminals often use virtual assets (VAs) to move large sums quietly. The report explains how cybercriminals launch ransomware, launder payments, and detect risk indicators. These indicators help organizations spot and prevent ransomware-related suspicious transactions. In Uganda, cybercrime is a critical issue. During the 2023/2024 financial year, 245 cases were reported, a 14.3% decrease from 286 in 2022. Despite this, financial losses exceeded **1.5 billion** UGX (**UGX 1,543,292,161**) in 2023, with only **UGX 377,441,465** recovered (Barigye, 2024).

Cybercrime often relies on data to execute attacks, highlighting the need for stronger encryption (methods for making data unreadable without authorized access) for data in transit (data being moved between devices) and at rest (data stored on systems). Enhanced data encryption further secures sensitive information against cyber threats and helps prevent data compromise, thus supporting a secure UDM. Security training (educational activities to increase staff awareness of cyber risks) strengthens an organization's resilience against attacks. It ensures protection for personal, organizational, financial, and digital data, whether at rest or in transit (Madnick, 2023). The significance of this paper is that securing Unified Data Models (UDMs) for Cyber-Physical Systems (CPS) is essential, as it safeguards sensitive information, ensures system reliability, and fosters trust, ultimately encouraging the adoption and innovation of trustworthy CPS.

2.1 Data Security Modelling Approaches include

Threat modelling is a process of identifying, analysing, prioritising, and mitigating cybersecurity threats and their associated vulnerabilities in a system or network (Naik et al., 2024). Various data modeling approaches for security are available, such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). It identifies threats to data in transit (tampering, information disclosure) and in storage (spoofing, elevation of privilege). While it provides a strong, comprehensive threat categorization, implementation can be challenging. Attack Tree analyzes vulnerabilities in both transit and storage, visualizing attack paths (strength), but it can be resource-intensive (weakness). DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) has limited focus on transit and storage details;

it is straightforward for risk prioritization (strength) but less thorough (weakness). CIA (Confidentiality, Integrity, and Availability) safeguards confidentiality and integrity during transit, as well as availability, with integrity maintained in storage. It is based on fundamental security principles (strength), but requires detailed implementation (weakness).

However, other threat data modeling techniques included PASTA, an acronym for Process for Attack Simulation and Threat Analysis. Its key feature is threat modelling, with collaboration, attack simulation, and risk assessment. PASTA use is complex and scalable; it is applicable in large organizations that need an organizational risk assessment method. OCTAVE, an acronym for Operationally Critical Threat, Asset, and Vulnerability Evaluation, has a key feature that focuses on threat modeling and collaboration, along with organizational risk assessment. OCTAVE use is complex; it is moderately scalable, applicable to organizations that require cross-team collaboration and an organizational risk assessment, and LINDDUN, an acronym for Link-ability, Identifiability, Nonrepudiation, Detectability, Disclosure of information, Unawareness, and Noncompliance, that focuses on threat modeling privacy threats. It is complex, scalable, and applicable in organizations that require privacy risk assessment and management (Naik et al., 2024).

2.1.1 Stages of Data Security Risks in Unified Data Models for CPS

This paper proposes an acronym **SUSDE model** for securing the Unified Data Model in Cyber-Physical Systems**,** where SUSDE letters represent the potential stages where the attack on data may occur as follows.

S – Sources of Data Ingestion: It refers to data from different sources encountered during transit to the unification point (e.g., interception or tampering).

U – Unification Process: It refers to data that may be exposed to threats such as unauthorized access, tampering, or breaches during integration or processing.

S – Storage (Unified Data Model Repository): It refers to stored unified data that may be subject to threats such as unauthorized access, data breaches, or privilege escalation attacks.

D – Data Transit (post-unification): It refers to unified data moving to other systems, applications, or users that can be targeted (e.g., interception, tampering, information disclosure).

E – End User Access: It refers to Data accessed by end users that can be vulnerable to unauthorized access, data leakage, or phishing attacks.

Identifying these stages in the unified data model is important to determine the most reliable strategy to prevent data compromise at all stages of the Data Unification process.

2.1.2 Comparative analysis to prevent threats at each stage in the UDM

Data in a unified model faces threats at different stages. During **data ingestion from sources**, risks include interception, tampering, and spoofing, which are addressed through encryption (TLS), authentication, and integrity checks. In the **unification process**, risks include unauthorized access, tampering, and breaches, which are mitigated by access controls, encryption, and monitoring. **Storage (the unified data model repository)** is vulnerable to unauthorized access, breaches, and privilege escalation, protected by encryption at rest, access controls, and anomaly detection. **During data transit (post-unification)**, threats include interception, tampering, and information disclosure, which are mitigated through encryption (TLS) and secure protocols. At the **end-user level**, risks include unauthorized access, data leakage, and phishing, which are mitigated through authentication, authorization, data masking, and user training.

The comparison of threat prevention across stages shows that encryption is crucial for securing data at every point. Encryption, a core cybersecurity technique, plays an essential role in protecting digital information from unauthorized access and potential breaches (Goyal et al., 2022).

2.1.3 Different forms of threats and solutions on Unified Data Model for CPS

In Unified Data Models (UDMs) for Cyber-Physical Systems (CPS), attacks can happen at different stages. During Data Ingestion, interception captures data in transit, tampering modifies data, and spoofing injects fake data. In the Unification Process, unauthorized access and privilege escalation pose risks. Storage can face breaches and disclosure of sensitive information. During Data Transit, interception and tampering pose a threat to data security. At End User Access, unauthorized access remains a concern.

The Data Spoofing Encryption (DSE) algorithm normalizes data to prevent the attacker from learning about it, thereby preserving data privacy (Makasiranondh et al., 2024).

Encryption ensures data remains safe, even if it is intercepted (Mubeen et al., 2022). Frequent security awareness training and implementation of robust authentication systems, strategies to avoid illegal data access (Mubeen et al., 2022).

2.2 Research Gap

The research gap is the absence of a secure unified data model for Cyber-Physical Systems (CPS) that effectively ensures data security in transit and at rest for end users.

This paper aims to fill this gap by designing and testing a secure unified data model for CPS end-users that emphasizes confidentiality, integrity, and availability of sensitive data. By providing a secure data model for Unified Data for CPS, the paper supports the development of more trustworthy and resilient implementations of secure Unified Data Models in CPS.

2.3 Problem

Unified Data Models (UDMs) in Cyber-Physical Systems (CPS) face significant data security threats, risking the integrity and confidentiality of sensitive information in data transit and at rest. While UDMs enhance interoperability, they also increase vulnerability to threats such as breaches and unauthorized access, which can undermine CPS reliability and trust. Implementing a Secure UDM framework is crucial. This framework strengthens access controls, encryption, and anomaly detection, effectively reducing risks and improving CPS data security. Consequently, it enhances system reliability and fosters trust in CPS applications.

Although UDMs can enhance CPS security, trust, and privacy through standardized management (Busari & Bello, 2024), their implementation also introduces significant data security risks. This highlights the need for a Secure UDM framework to balance interoperability with protection.

High security risks are present for data in transit and at rest. Strong security measures defend against cyber threats. In 2022, global cyberattacks accounted for 38% of incidents (Nahla Davies, 2023).

3.0 Methodology

3.1 Methodology to Investigate Data Security Risks Associated with the Unified Data Model in Cyber-Physical Systems

The methodology involved a literature review that identified potential vulnerabilities through threat modeling and risk assessment frameworks, analyzing data security risks to the Unified Data Model in Cyber-Physical Systems. The review helped us understand the current state of data modeling in CPS. Recent studies emphasize the importance of considering security and interoperability in CPS data models (Wang et al., 2021).

Securing a Unified Data requires analyzing several threat modeling approaches on data, then selecting the most appropriate method for protecting Unified Data in Cyber-Physical Systems. This includes robust encryption, access controls, security training, and regular assessments. The approach in this study aims to secure unified data both in transit and at rest.

4.0 Findings

This paper categorizes the stages of the unified data model, identifies vulnerabilities and breaches at each stage, and outlines the most appropriate preventive measures for the identified risks. The comparison strongly emphasizes data encryption as the most appropriate technique for securing data at each stage of data unification, alongside other data protection measures. There is a need to explore the strengths and weaknesses of encryption to advance robust data encryption that ensures reliable security and privacy in Unified Data Models for CPS.

Table 1: Analysis showing the relevance of encryption at each stage of Unified Data Models to secure data for Cyber Physical Systems.

	Stages in UDM	Forms of Attack	Possible Solution
1	Sources of Data Integration	Interception, tampering, spoofing	Encryption (TLS), Authentication, integrity checks
2	Unification Process	Unauthorized Access, tampering, breaches	Access controls, encryption, monitoring/auditing
3	Storage (Unified Data Model Repository)	Unauthorised Access, data breaches, elevation of privilege	Encryption at rest, access controls, anomaly detection
4	Data Transit (post-unification)	Interception, tampering, and disclosure of Information	Encryption (TLS), secure protocols (like HTTPS), and integrity checks
5	End User Access	Unauthorized access, data leakage, phishing	Authorization, authorization, data masking, user training

The description of Table 1 above is as follows.

Each stage in the data unification process has various forms of data security attacks, and it is evident that advances in data encryption are core for securing data in Unified Data Models, in addition to other data security measures.

Table 2: Analyzes seven (7) Data Security Approaches for Data Threat and Risk comparison.

SNo.	Approach	Description	Data Transit	Data Storage	Strength	Weakness
1	**STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)	A threat model for identifying computer security threats	Explicitly identifies threats during transit (such as tampering or information leaks)	Explicitly identifies storage threats (e.g., spoofing, elevation of privilege)	Comprehensive Threat Classification	It can be challenging to apply
2	**Attack Tree**	A method for security threat modeling using dependency analysis.	Explicitly examines transit vulnerabilities	Explicitly examines storage vulnerabilities	Displays the attack path	Possibly resource-intensive
3	**DREAD**	Classification system for security threats	Partially addresses transit-specific threats.	Partially addresses storage-related threats	Has a straightforward risk prioritization.	More limited
4	**CIA** (Confidentiality, Integrity, Availability)	A Security Model for Building Security in Information Technology Systems	Explicitly guarantees confidentiality during transfer.	It guarantees availability and data integrity in storage.	Provides fundamental security principles	High-level; requires implementation details.
5	**PASTA**	A process for assessing security threats	Explicitly analyzes transit threats in the process context	Explicitly analyzes storage threats in the process context	Business-oriented risk assessment	Needs process expertise.
6	**OCTAVE**	Risk-based security evaluation	Explicitly addresses transit risks	Explicitly addresses storage risks	Organizational risk focus	It can be complex to implement
7	**LINDDUN**	Privacy threat modeling	Explicitly identifies transit privacy threats	Identifies threats to storage privacy.	Comprehensive privacy focus	Focuses on privacy rather than all security threats

The description of Table 2 above is as follows.

STRIDE thoroughly identifies threats to both data in transit and at rest (such as tampering, spoofing, and elevation of privilege), making it a strong choice for securing unified CPS data. Unlike CIA, which emphasizes high-level security principles (confidentiality, integrity, availability) but does not specify threat identification, STRIDE offers actionable threat categorization for CPS environments.

While STRIDE's comprehensive threat categorization makes it a strong fit for Unified Data Models (UDMs) in Cyber-Physical Systems (CPS), other models have limitations. DREAD emphasizes risk prioritization with limited transit and storage details. Attack Trees examine vulnerabilities but are resource-intensive. PASTA requires process expertise and is business-focused, while OCTAVE's organizational risk focus makes implementation complex. LINDDUN prioritizes privacy threats but does not address all security concerns.

5.0 Conclusion

Securing Unified Data Models (UDMs) in Cyber-Physical Systems (CPS) involves addressing threats at all stages, including ingestion, unification, storage, transit, and access. STRIDE's comprehensive threat model effectively identifies risks such as interception, tampering, spoofing, breaches, and unauthorized access. Applying STRIDE with mitigations like encryption, access controls, and monitoring can enhance CPS data security.

References

Alexandre Diard. (2025, May 25). *How to Advance Your Organization with Unified Data Models*. Https://Peoplespheres.Com/How-to-Advance-Your-Organization-with-Unified-Data-Models/.

Barigye, C. (2024). *Strengthening Cyber Safety and Ransomware Response | Financial Intelligence Authority*. Press Release July 19, 2024. ICT Systems and Security Director at Finance Intelligence Authority (FIA). https://www.fia.go.ug/strengthening-cyber-safety-and-ransomware-response

Busari, W. A., & Bello, A. A. (2024). Security, Trust, and Privacy in Cyber-physical Systems (CPS). *Proceedings of the 2024 2nd International Conference on Cyber Physical Systems, Power Electronics and Electric Vehicles, ICPEEV 2024*. https://doi.org/10.1109/ICPEEV63032.2024.10932087

Goyal, P., Sharma, P., & Sharma, M. (2022). The importance of data encryption in data security. *Jnao-Nu.ComP Goyal, P Sharma, M Sharma, A PareekJournal of Nonlinear Analysis and*

Optimization, 2022•jnao-Nu.Com, *13*(1). https://doi.org/10.36893/JNAO.2022.V13I02.001-011

Li, F., Wu, X., & Han, H. (2025). Data-Driven Cyber Physical Systems. *Data-Driven Cyber Physical Systems*. https://doi.org/10.1007/978-981-96-8709-1

Madnick, S. E. (2023). *The continued threat to personal data: Key factors behind the 2023 increase*. https://www.apple.com.cn/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf

Makasiranondh, W., & … S. A. (2024). A Data Spoofing Encryption Algorithm for Data Security and Data Privacy. *Ieeexplore.Ieee.OrgW Makasiranondh, S Angsirikul, A Aribarg2024 8th International Conference on Information Technology (InCIT), 2024•ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/10810622/

Mubeen, M., Arslan, M., & Communication, G. A. (2022). Strategies to Avoid Illegal Data Access. *Academia.EduM Mubeen, M Arslan, G AnandhiJournal of Communication Engineering & Systems, 2022•academia.Edu*. https://www.academia.edu/download/111172139/29_40StrategiesToAvoidIllegalDataAccess.pdf

Nahla Davies. (2023, May 29). *Should You Consider a Unified Data Model?* https://www.dataversity.net/should-you-consider-a-unified-data-model/

Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., & Song, J. (2024). A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. *Lecture Notes in Networks and Systems*, *884 LNNS*, 271–280. https://doi.org/10.1007/978-3-031-74443-3_16

Zubin et al. (2025, May 22). *Unified or Siloed? Exploring the Best Strategies for Effectively Managing Your Data Resources.* https://www.datadynamicsinc.com/blog-unified-or-siloed-whats-the-best-way-to-manage-your-data/