Available online at www.rajournals.in

RA JOURNAL OF APPLIED RESEARCH
ISSN: 2394-6709
DOI:10.47191/rajar/v10i07.03
Volume: 10 Issue: 07 July-2024

International Open Access

Impact Factor- 8.174

Page no.- 145-160

Enhancing Confidentiality and Privacy of Data in Motion from Embedded Systems

Ahamya William[1], Drake Mirembe[2], Evarist Nabaasa[3]
[1,3]Mbarara University of Science and Technology
[2]College of Computing and Information Sciences, Makerere University

ARTICLE INFO

Published Online:
26 July 2024

ABSTRACT

Data has become the new "oil" and is a drive for the knowledge based digital economy. Like any asset of a value, data has numerous security related challenges associated with its integrity, confidentiality and availability. Furthermore, emerging computing paradigms such as cloud and grid computing are enlarged the physical foot print of data in a given system, hence creating new challenges associated to data security. The new computing technologies such as wireless sensor networks and their applications in various fields present new challenges associated with Data Confidentiality and Privacy. Thus, this study aimed at improving confidentiality and Privacy of data in motion in wireless Vehicle Sensors.

The study used design science philosophy and applied inductive research strategy, since it aims at providing a solution to an issue in a unique domain whose problem and solution are entwined. To address objectives one, a mixed methods approach was used that involved both qualitative and quantitative methods of data collection and analysis. The design of the framework was modeled using a Unified Modeling Language. The research revealed that there is existence of data from the embedded systems used without clients' consent. It was also revealed that enhancing confidentiality and privacy of data in motion in embedded systems save organizations from financial loss. The study identified several major weaknesses and vulnerabilities in existing frameworks, including lack of end user awareness, cyber threats, breaches in data in motion, gaps in data frameworks, human errors, limited knowledge and access to data frameworks, insecure file sharing, and potential malicious actions or third-party infiltration. Basing on the above findings, a framework to enhance confidentiality and privacy of data in motion was designed.

The framework proposed herein, creates a robust shield around data, elevating security standards and instilling trust in the system's ability to safeguard sensitive information. Through meticulous attention to authorization, consent management, integrity verification, and abuse detection, the framework stands poised to elevate data security standards and foster trust in the system's ability to safeguard sensitive information. The study findings suggest that the framework for enhancing confidentiality and privacy of data in motion is perceived as effective and efficient by the respondents. This positive feedback underscores the importance of using the ECPDM framework to safeguard embedded data in motion.

Corresponding Author:
Ahamya William

1.0 BACKGROUND AND CONTEXTUAL

Embedded systems have a rich history dating back to the 1960s, with early developments like Stark Charles Draper's integrated circuit for the Apollo Guidance computer (Brock & Lécuyer, 2020). These systems evolved over the years, finding applications in diverse fields, including the Minuteman missile guidance system and the automotive industry, where microprocessors were integrated into vehicles like the Volkswagen 1600 (Ahmad et al., 2019).

The 1970s witnessed a significant drop in the price of integrated circuits, leading to widespread adoption (Brock & Lécuyer, 2020). Texas Instruments developed the first microcontroller in 1971, marking a milestone in embedded system technology. Intel's 8008 and 8080 series further advanced with increased memory capacities. The late

1980s saw the introduction of the first embedded operating system by Wind River, followed by Microsoft's Windows Embedded CE in 1996. By the late 1990s, embedded Linux gained popularity and is now ubiquitous in various devices (Qin et al., 2018; Rouget et al., 2017).

In contemporary times, the prevalence of mobile and IoT devices has led to a surge in data breaches and cyber-attacks. Data has become the new "oil," driving the knowledge-based digital economy (Ahmad et al., 2019).

Businesses globally are expanding rapidly due to the explosion of Information and Communication Technology (ICT) innovations (Cheryl et al., 2021; Kim et al., 2017; Naveed et al., 2018) Additionally, companies world over are largely supported and driven by Information Systems (IS); on the other hand, protecting sensitive information, valuable assets and intellectual property in the organizations against external and internal attacks becomes more sophisticated and difficult than ever before (Solms & Niekerk, 2013; Martin & Rice, 2011). As one of the key dimensions of Information Technology (IT), information security focus on protecting information from a wide range of threats in order to ensure business continuity, minimize business risks, and maximize the return on investments as well as business opportunities (Cheryl et al., 2021; Kim et al., 2017; Naveed et al., 2018).

Different regions have tried to handle data generation and management in various ways. North America, particularly the United States, continues to be a global leader in data generation and management (Dutta, 2021). Silicon Valley and technology hubs drive innovation and technological advancements (Adler & Florida, 2021; Marchesani,2021). Europe places a strong emphasis on data privacy and protection, as demonstrated by the General Data Protection Regulation (GDPR) (Kuner, 2021; Yeung & Bygrave, 2021; Streinz, 2021). The region is also investing in technologies like block chain for secure data management (Teodorescu & Korchagina,2021; Babenko,2020). The Asia-Pacific region, including countries like China, Japan, and South Korea, is experiencing rapid technological growth (Li et al., 2021; Usman & Hammar, 2021). China, in particular, is a significant player in data generation and AI development (Gamito, 2023; Sheehan, 2021; Borgogno, & Savini-Zangrandi, 2024). Latin America is seeing increased digitization and data generation, driven by factors like mobile technology adoption and e-commerce growth (Cepal, 2022; Beylis,2023). Data management practices are evolving, but there are still challenges in some areas. Africa is experiencing a digital transformation with the increasing availability of affordable smartphones and internet connectivity (African Union, 2020; Nwokolo et al.,2023; Kamel, 2021). This is leading to a surge in data generation, particularly in mobile applications, e-commerce and Sensors and devices connected to the internet (embedded systems) (Teevan & Domingo, 2022; Ali & Xia, 2022; Lay & Tefese, 2023).

Given the escalating data volume and the growing menace of cyber threats, the significance of cybersecurity has reached a paramount level. In response to this pressing concern, international legal instruments have emerged as pivotal components in safeguarding data privacy and security on a global scale (United Nations, 2016). These instruments essentially serve as a foundation, offering countries a structured framework to institute laws and regulations (Bennett & Raab, 2017). Through these legislative measures, the protection of individuals' personal data is fortified, concurrently fostering secure data practices (Fiero & Beier, 2022). Several key international legal instruments contribute to the protection of data privacy and security. One significant instrument is the General Data Protection Regulation (GDPR) implemented by the European Union (EU) (Verdoodt et al., 2023; Fiero & Beier, 2022; European Union, 2018). The GDPR sets out comprehensive rules for the processing and protection of personal data within the EU and applies to organizations that handle EU citizens' data, regardless of their location (Dove & Chen, 2021). It establishes principles for data collection, consent, and individuals' rights, such as the right to access and rectify their data. The GDPR also imposes strict obligations on organizations to implement appropriate technical and organizational measures to ensure data security (Verdoodt et al., 2023).

Another important instrument is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108 (De Terwangne,2021; 2022; Goral, 2021). This Council of Europe treaty aims to safeguard individuals' rights and fundamental freedoms concerning the processing of personal data (De Terwangne,2021; 2022). It establishes principles for data protection, including fair and lawful processing, purpose limitation, and security measures (Bennett, 2020). Convention 108 also promotes international cooperation in data protection matters and encourages countries to establish national data protection authorities (Botin & Mari, 2021).

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework is another significant instrument that promotes data privacy and security in the Asia-Pacific region (APEC, 2005; 2015). It provides a set of principles and guidelines for member economies to develop and implement privacy protection policies (APEC, 2005; 2015). The framework emphasizes the importance of individual control over personal information, accountability of organizations, and cross-border data flows with appropriate safeguards. It encourages member economies to adopt privacy laws and establish enforcement mechanisms to ensure compliance (APEC, 2005; 2015).

Additionally, the United Nations General Assembly

adopted the Resolution on the Right to Privacy in the Digital Age (UNGA, 2013). This resolution recognizes the importance of protecting individuals' privacy rights in the context of rapidly advancing technology Age (UNGA, 2013). It calls on member states to review and update their legislation to ensure the protection of privacy rights and to cooperate in addressing privacy challenges at the international level Age (UNGA, 2013). In the United States, data privacy regulations and laws are governed by a combination of federal and state laws. The California Consumer Privacy Act (CCPA) grants California residents certain rights regarding their personal information (California Legislative Information, 2018). The Health Insurance Portability and Accountability Act (HIPAA) sets standards for the protection of sensitive health information (U.S. Department of Health & Human Services, 1996.). Financial institutions are subject to the Gramm-Leach-Bliley Act (GLBA), which requires them to protect the privacy and security of customers' personal financial information (Federal Trade Commission, 1999). The Children's Online Privacy Protection Act (COPPA) regulates the collection of personal information from children under the age of 13 (US Federal Government, 1998). The Fair Credit Reporting Act (FCRA) governs the collection, use, and disclosure of consumer credit information (Federal Trade Commission, 1998). The Electronic Communications Privacy Act (ECPA) sets standards for the protection of electronic communications (U.S. Department of Justice, 1986).

Data privacy and protection instruments in Africa play a crucial role in safeguarding individuals' personal information and promoting secure data practices across the continent (Prinsloo & Kaliisa,2022; Hlomani & Ncube, 2023; Greenleaf & Cottier, 2023). Several countries in Africa have enacted data protection laws and regulations to address the growing concerns surrounding data privacy and security (Swale, 2021). For example, South Africa has the Protection of Personal Information Act (POPIA) of 2020, which establishes principles for the lawful processing of personal information and grants individuals certain rights over their data (Netshakhuma,2020). Nigeria has the Nigeria Data Protection Regulation (NDPR) (2019), which sets out guidelines for the protection of personal data and imposes obligations on organizations that process such data (Akintola, & Akinpelu,2021). Additionally, Kenya has the Data Protection Act (2019), which aims to protect individuals' privacy rights and regulate the processing of personal data (Kevins & Brian, 2022). These instruments provide a legal framework for data protection, ensuring that individuals' personal information is handled responsibly and securely. They also contribute to building trust in digital transactions and fostering a culture of data privacy and security in Africa.

Uganda has taken steps to address data privacy and security by enacting the Data Protection and Privacy Act in 2019. This act aims to protect the privacy of individuals' personal data and regulate its processing within the country (National Information Technology Authority, 2019). It aligns with international best practices and standards, ensuring that Uganda is in line with global efforts to safeguard data privacy (Republic of Uganda, 2019). The Data Protection and Privacy Act establishes principles and requirements for the collection, processing, and storage of personal data (Grant Thornton Uganda, 2019). It emphasizes the importance of obtaining informed consent from individuals before their data is collected and processed (Grant Thornton Uganda, 2019). The act also grants individuals the right to access and correct their personal data, giving them control over their information (Data Protection Laws of the World, 2019). Under this act, organizations that process personal data are required to implement appropriate technical and organizational measures to ensure data security (Grant Thornton Uganda, 2019). They must take steps to protect personal data from unauthorized access, disclosure, alteration, or destruction (Republic of Uganda, 2019). The act also mandates the reporting of data breaches to the relevant authorities and affected individuals, ensuring transparency and accountability in the event of a security incident (Republic of Uganda, 2019; National Information Technology Authority, 2019).

Despite the legal framework, data breaches, ransomware attacks, and other cyber threats still pose significant risks to data integrity and privacy(Etemadi et al., 2021; Lu & Xu, 2019). Like any valuable asset, data faces numerous security challenges related to its integrity, confidentiality, and availability. Data confidentiality is uncompromised both at motion and at rest if it is accurate, complete, and consistent throughout its entire lifecycle (Ahmad et al., 2019). Despite the critical importance of safeguarding data privacy, various bad actors continue to gain unauthorized access to data in motion and at rest from embedded systems due to deficiencies in existing approaches to data privacy management (Koziolek et al., 2020). According to Sanchez (2021), growing breaches of data privacy are largely attributed to negligent employees or contractors (48%), third-party mistakes (41%), external attacks (27%), and malicious insiders (5%). The current approaches to safeguarding data privacy are characterized by weak or inadequate controls for user content management (Reilly, 2021).

This escalating threat landscape necessitates a focused investigation, particularly in the context of vehicle tracking embedded systems. The study specifically addresses the challenge of unauthorized access and use of personal data in these systems, especially in the transmission of vital information through collaboration platforms like Slack, which poses a significant risk of

exposure to unauthorized users (Mallmann et al., 2018). Existing frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, HIPAA, PCI DSS, and CIS Controls provide valuable guidelines for managing cybersecurity risks (Lin & Lee, 2021a, 2021b). However, these frameworks lack systematic approaches to address unauthorized access to data in motion, particularly in terms of user notification and consent (Qin et al., 2018; Saad, 2021). The gaps in the existing frameworks that necessitated this study include the lack of robust security measures, inadequate encryption algorithms, insufficient secure communication protocols, limited data anonymization techniques, increasing challenges in data protection, and deficiencies in existing approaches to data privacy (Saad, 2021). Addressing these gaps is crucial to enhance the security and integrity of data in motion within vehicle tracking embedded systems (Alqahtani, & Kumar, 2024; Sadaf, 2024; Krichen, 2023). The study aims to fill this gap by developing a Data in Motion Privacy Enhancing Framework, focusing on minimizing unauthorized access and use of personal data in vehicle tracking embedded systems through effective user notification and consent mechanisms.

2.0 PROBLEM STATEMENT

Data has become a valuable asset in the knowledge-based digital economy, often referred to as the new "oil." However, the increasing value of data also brings numerous security challenges related to its integrity, confidentiality, and availability (Natumanya et al.,2021). To ensure data confidentiality, it is crucial that data remains accurate, complete, consistent, and protected throughout its entire lifecycle, as envisioned by its owner globally (Ahamya, Mirembe & Nabasa, 2021). Unfortunately, existing approaches to data privacy management in embedded systems have proven to be deficient, allowing unauthorized access to data both in motion and at rest (Ahamya et al., 2021; Kolinsky, 2021). This has led to growing breaches of data privacy, as highlighted in a study conducted by Sanchez (2021). The study revealed that negligent employees or contractors accounted for 48% of data privacy breaches, followed by third-party mistakes at 41%, external attacks at 27%, and malicious insiders at 5% (Sanchez, 2021).

The current approaches to safeguarding data privacy in vehicle tracking embedded systems suffer from weak or inadequate controls for user content management, leaving data in motion vulnerable to unauthorized access and compromise (Lin & Lee, 2021a, 2021b). These deficiencies in data privacy management pose significant risks to individuals, organizations, and even businesses (Pezeshki et al., 2020). Therefore, there is an urgent need to address these challenges and develop robust approaches to safeguard data privacy in embedded vehicle tracking systems. Thus, this study seeks to improve confidentiality and privacy of data in motion in wireless Vehicle Sensors (Alqahtani, & Kumar, 2024; Sadaf, 2024; Krichen, 2023). This research aims to bridge the gaps in existing data privacy management approaches by proposing a comprehensive framework that ensures data confidentiality in motion. The framework will incorporate strong controls for user content management, encryption algorithms, secure communication protocols, and data anonymization techniques to protect vehicle tracking data from unauthorized access and compromise.

3.0 OBJECTIVES

The following objectives guided the study;

1. Establish limitations of the existing data security frameworks and determine the ideal requirements for a pragmatic data in motion confidentiality and privacy framework.
2. Design a data in motion confidentiality and privacy enhancing framework.

4.0 LITERATURE REVIEW

4.1 Overview of Data in Motion

Data in motion also referred to as "data in transit", is digital information transferred between locations, either within or between computer systems (Pourrahmani et al., 2023; Oladimeji et al., 2023; Syed et al., 2022). Data in motion can be data sent from desktop computer to the cloud infrastructure, portable devices, or other exit points (Debauche et al., 2022; Arikumar et al., 2022). Once such data arrives at its final destination, it is classified as "data at rest" (Khujamatov et al., 2022; Shaik, 2022). Data in motion must be safeguarded not only because of a growing number of regulatory data processor compliance requirements both nationally and internationally, but to avoid exposure to possible financial losses and penalties as well as reputational risks (Qinn, 2021; Debauche et al., 2023). When data is in motion it is exposed to many risks; as data travels, both inside and outside the organization infrastructure, it can easily be accessed by unauthorized entities (Riggs et al., 2023; Lehto et al,2022). When in motion, data has to contend with wide range of threats, including network failures, human error, insecure file sharing, malicious actions, and more (Alshurideh et al., 2023; Lehto et al, 2022).

Interestingly, there is undoubtedly a continuous growing security concern over the exposure of information and data during its entire life cycle (Omolara et al., 2020). The high constant level of connectivity coupled with low-cost bandwidth and motion propagates unauthorized and malicious users both within and without the organizations to access and monetize valuable information such as medical records, intellectual properties, security secrets and national secrets, among others (Ettredge et al., 2018;

Frangopol & Liu, 2019; Mohandu & Kubendiran, 2021).

In the contemporary landscape, data security has transcended its status as a mere financial concern to emerge as a pivotal facet of comprehensive data life cycle management (Murti, 2022). This cost encompasses not only monetary considerations but encapsulates the intricacies of processes, procedures, and the human element engaged in the overarching information and data life cycle. Various protocols have been established to fortify the security of data during its transit and while at rest. Notable among these is the deployment of the Hypertext Transfer Protocol Secure (HTTPS), which stands as a secure conduit for transmitting data between web servers and browsers during online interactions (Manickam et al., 2019). For secure digital communication, the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol has been instrumental, facilitating the sending of digitally signed and encrypted messages (Schwenk, 2022). Additionally, the use of virtual private networks (VPNs) has gained prominence in creating secure connections between computing devices and computer networks, or between two networks, especially when traversing insecure communication mediums like the public Internet (Ezra et al., 2022). These technologies collectively serve as conduits through which information is conveyed, strategically minimizing the compromise of both information and data integrity, whether at rest or in motion (Qinn, 2021; Debauche et al., 2023; Mohandu & Kubendiran, 2021; Lehto et al,2022).

In the realm of non-homogeneous or heterogeneous technological environments (Wlosinski, 2018), as exemplified in the Embedded System (ES), this study assumes a pivotal role. The objective is to establish a secure environment that mitigates the compromise of data integrity in motion within the Embedded System. By navigating the diverse technological landscape inherent in embedded systems, this study aspires to contribute to the creation of a fortified and secure framework. This framework aims not only to uphold the integrity of data but also to address the multifaceted challenges presented by the dynamic interplay of technologies within the Embedded System.

4.2 Overview of Embedded Systems

Embedded systems are special-purpose computing systems embedded in application environments or in other computing systems and provide specialized support (Yamamoto et al., 2019; Barbirotta, 2023). The decreasing cost of processing power, combined with the decreasing cost of memory and the ability to design low-cost systems on chip, has led to the development and deployment of embedded computing systems in a wide range of application environments (Li et al., 2019). Examples include network adapters for computing systems and mobile phones, control systems for air conditioning, industrial systems, and cars, and surveillance systems (Huda et al, 2024). Embedded systems for networking include two types of systems required for end-to-end service provision: infrastructure (core network) systems and end systems (Kabashkin, 2023). According to Tud et al (2024), the first category includes all systems required for the core network to operate, such as switches, bridges, and routers, while the second category includes systems visible to the end users, such as mobile phones and modems.

Any embedded system will vary based on the application and industry it serves. Whether it's in consumer electronics, automotive control, healthcare devices, industrial automation, or other domains, these general principles guide the development of effective embedded systems (Murti, 2022). It is worth noting that most of the embedded systems commonly used today in various fields are commonly those devoted to perform keen and explicit responsibilities, and these mostly exist in several items of life, for instance, mobiles, ACs, toys and washing machines (Tud et al., 2024; Saha, 2022). Most of these embedded systems have a micro-controller that get input from the existing peripherals especially buttons, the keypads or any other form of sensors that give out-put through available display, motor as well as any other form of mechanical work. Sometimes, these forms of systems have external memory storing non-volatile data, as well as building into the micro-controller (Gill et al, 2024). Embedded systems are largely categories into two, based on either microcontroller performance or function requirements (Perez et al., 2023; Rehman, 2018).

Figure 2.1 below illustrates the classification of the embedded systems

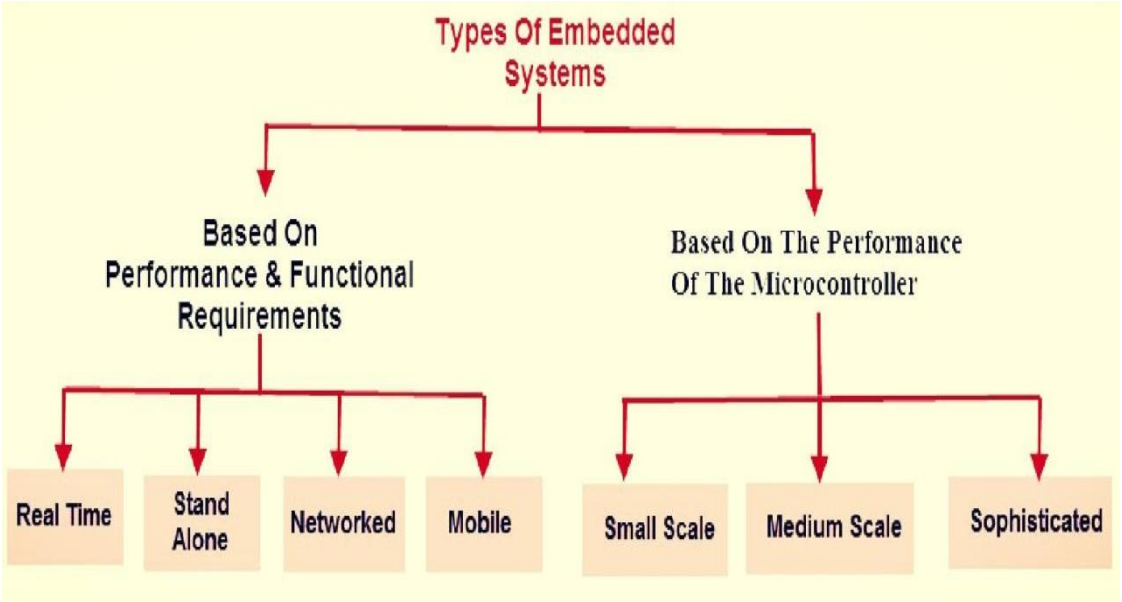


Figure 2.1: Showing the different types of embedded systems
Adopted from Rehman, (2018)

4.3 Vehicle Tracking Embedded Systems

Vehicle tracking embedded systems are specialized devices or software solutions that are designed to track and monitor the location and movement of vehicles in real-time (Conrad, 2024; Rath et al.,2024). These systems utilize a combination of technologies, such as GPS (Global Positioning System), wireless communication, and microcontrollers, to collect and transmit data about the vehicle's location, speed, and other relevant information (Etezadi & Eshkabilov, 2024; Ranjan, 2022; Lo et al.,2024; Shama & Mehra, 2023).

Vehicle tracking embedded systems typically consist of a tracking device that is installed in the vehicle, which is connected to a network (Lo et al.,2024; Shama & Mehra, 2023). The tracking device uses GPS technology to accurately determine the vehicle's location. This information is then transmitted to a central server or cloud-based platform using wireless communication technologies, such as GSM (Global System for Mobile Communications) or other cellular networks (Chen et al, 2023; Lo et al; 2024).

Users can access the tracking data through a web-based interface or mobile application, allowing them to monitor the vehicle's location and movement in real-time. This information can be used for various purposes, including fleet management, logistics optimization, theft prevention, and driver behavior monitoring (Shihag et al.,2023; Krishnamoorthy et al.,2023).

Vehicle tracking embedded systems offer numerous benefits, including improved operational efficiency, enhanced security, and better customer service (Etezadi & Eshkabilov, 2024; Ranjan, 2022). They enable businesses to track and manage their vehicles effectively, optimize routes, monitor driver performance, and ensure timely deliveries (Shama & Mehra, 2023). Additionally, these systems can provide valuable insights and data analytics that can be used for decision-making and process improvement (Singh et al.,2024).

It is essential to establish clear policies and guidelines regarding data usage and ensure compliance with relevant privacy regulations to address these concerns and maintain user trust and responsible use of these systems (Ahamya et al., 2023).

4.4 Existing Frameworks of Data Security in Vehicle Tracking Embedded Systems

Table 4.1: Showing the summary of weaknesses in some of the existing frameworks

Frameworks	Weaknesses
Hadoop framework	Deficiency of Native Security Features Minimal Authentication Mechanisms. Inadequate Authorization Controls. Limited Encryption Support. Complexity of Configuration. Limited Support for Data Masking and Redaction. Difficulty in Data Erasure No user consent
Endpoint Protector Framework	Dependency on Endpoint Agents Agent Compatibility Issues Overhead on Endpoints Limited Protection Against Advanced Threats Adjustment of Policies Encrypted Data Transmission Dependency on Regular Updates and Patching Poor mechanics of consent notification
ISO/IEC 27001 Framework	Limited Prescriptive Guidance Focus on Process, not Technology Heavy Emphasis on Documentation Periodic Audits Resource Intensive Implementation Focus on Information Security Management Dependence on Human Factors Poor mechanics of consent notification
NIST Cybersecurity Framework	Deficiency of Specific Privacy Emphasis Limited Guidance on Data Minimization Focus on High-Level Controls Resource Intensive Implementation Requires Strong Internal Expertise Log files and audits have only 30 days of storage. Complications with RBAC (Role Based Access System) Poor mechanics of consent notification
GDPR (General Data Protection Regulation) Framework	Operational Complexity and Interpretation Data Minimization and Retention Data Security Measures Third-Party and Vendor Management Data Protection Officer (DPO) Requirement Global compliance challenges Poor mechanics of consent notification.

CIS Controls (Center for Internet Security Controls)	Emphasis on Technical Controls Limited Emphasis on Privacy Not Industry-Specific Lack of Guidance on Data Subject Rights Dependence on Implementation Expertise Resource Intensive Implementation Focus on High-Level Controls Dependence on Regular Updates Poor mechanics of consent notification

Recognizing existing gaps in established frameworks, this research aims to bridge these deficiencies by proposing a novel framework that squarely addresses the challenge of "unauthorized access and misuse of data arising from lack of user awareness when their data is being used." The primary goal of this study is to create a comprehensive Data in Motion Privacy Enhancing Framework, specifically tailored to mitigate the prevalent issues related to unauthorized access and misuse of personal data within vehicle tracking embedded systems.

5.0 METHODOLOGY

5.1 Research Design

The selection of an appropriate research paradigm and research design is an important step for enabling reliable knowledge (Alshaikh, 2018). The section explains the phases of the research, the research design and strategy, literature reviews, case studies and survey designs used in the study.

This research was anchored on the design science approach. Design science is a research methodology that focuses on creating innovative solutions to practical problems (Mirembe, 2015; Carstensen & Bernhard, 2019). It involves the development and evaluation of artifacts, such as frameworks, models, or systems, to address specific challenges in a particular domain (Muntean et al., 2022). In this study, design science was employed to develop a data in motion privacy enhancing framework aimed at minimizing unauthorized access and use of personal data in vehicle tracking embedded systems (Carstensen & Bernhard, 2019). The design science approach involved several key steps. Firstly, a thorough understanding of the problem domain and the existing challenges related to data privacy in vehicle tracking embedded systems was gained through a literature review and expert interviews. This helped identify the specific requirements and objectives for the framework (Yasin et al.,2020; Lier et al., 2024; Natumanya, & Nabaasa, 2022; Nduhukire et al., 2023; Mirembe, 2015).

Next, the design and development of the framework took place. This involved conceptualizing the framework, defining its components and functionalities, and designing the necessary mechanisms to ensure data privacy (Gieb et al.,2024). The framework was iteratively refined and improved based on feedback and evaluation. Below summarizes the design science research process. The phases of the research are explained below.

Phase 1:

i. Identification of the weaknesses in existing frameworks and the requirements needed to improve confidentiality and privacy of data in motion

Phase 2:

i. Collect data through field studies by conducting interviews using structured and semi-structured questionnaires, observation guides and document analysis

ii. Analyse data collected to identify requirements for the framework

Phase 3:

i. Develop the proposed framework for confidentiality and privacy of data in motion

5.2 Sample Size Determination

The ever-increasing need for a representative statistical sample in empirical research has created the demand for an effective method of determining sample size. According to Katamba & Nsubuga (2014), sample size is the portion or subset of the total population. To address the existing gap, the study sample was selected using Krejcie & Morgan (1970) table in determining sample size to represent a cross section of people in this study. In this regard, out of 180 as target population, a sample size of 128 was considered. These included; eight (8) top managers and directors, twenty-five (25) experts (IT Professionals, Privacy Experts and Security Analysts) in car tracking and sensor installers, twenty (20) ordinary employees and seventy-five (75) FMS clients (End-Users or Data Owners). This enabled the researcher to get a variety of views and unbiased response which made the study findings more reliable and balanced.

Table 5.1: Sample size determination using Morgan's table

Category	Population by Category	Sample Size	Sampling Technique	Data Collection Tool
Top managers and directors	8	8	Purposive	Interview Guide
Experts in car tracking and sensor installers	30	25	Purposive	Interview Guide
Ordinary Employees	25	20	Purposive	FGD Guide
FMS Clients	117	75	Simple Random	Questionnaire
Total Population (Entire)	180	128		

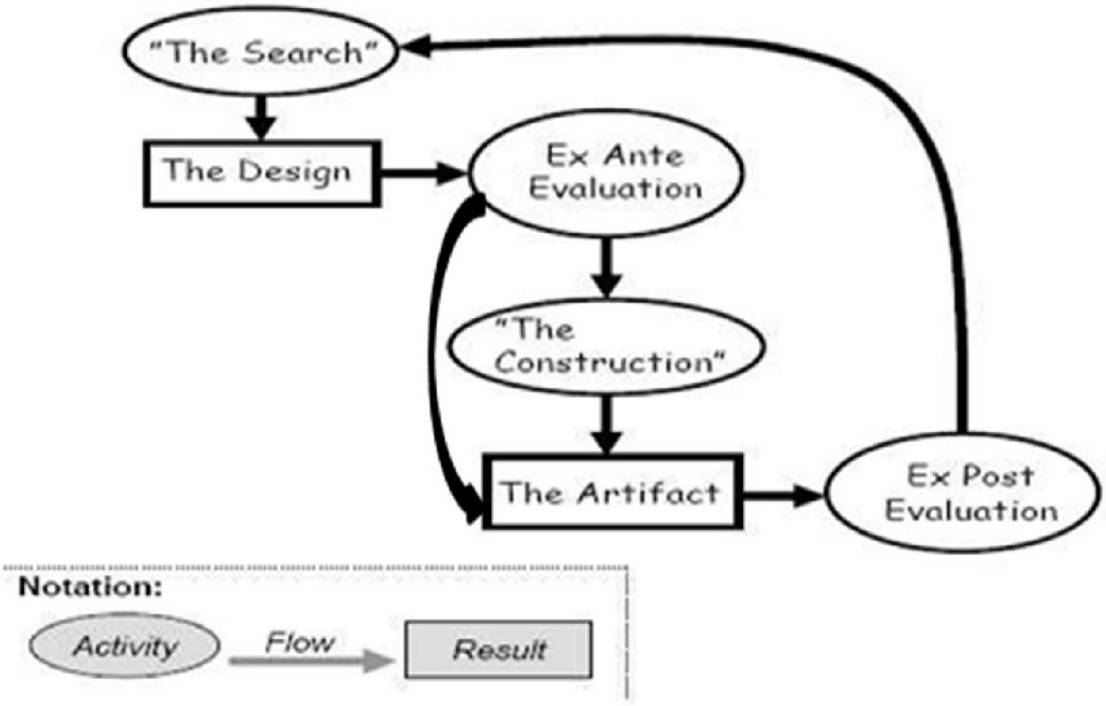
5.3 Design Science Approach

This research was conducted using the design science theory, a research methodology that focuses on creating innovative solutions to practical problems. The goal of design science is to develop and evaluate artifacts, such as frameworks, models, or systems, to address specific challenges in a particular domain. In this study, the design science approach was employed to develop a data in motion privacy enhancing framework for vehicle tracking embedded systems, with the aim of minimizing unauthorized access and use of personal data.

The figure below provides a visual summary of the design science research process, illustrating the iterative nature of the framework's design, development, and evaluation stages

Figure 5.1: Summarizes the design science research process

Adopted from Iterative design science research process (Baskerville, et al. 2009)



6.0 RESPONSE RATE

The sub section presents the summary of the statistics for the response rates. Details are presented in Table 4.1 below.

Table 6.1: Summary of study response rates

Category	Targeted respondents	No. actually involved	Percentage of response rate
Questionnaire			
FMS Clients	117	75	64.1%

Interviews			
Top managers and directors	8	8	100%
Experts in car tracking and sensor installers	30	25	83.3%
FGD Guide			
Ordinary Employees	25	20	80%
Total	180	128	71.1%

Source: Primary data, 2023

6.1 Existence of Confidentiality and Privacy of Data in Motion

The study focused on capturing the viewpoints of FMS clients regarding the presence of data confidentiality and privacy during its transition. Table 4.3 succinctly presents a summary of these perspectives through frequency and percentage distributions.

Table 6.2: Descriptive Results on the Existence of Confidentiality and Privacy of Data in Motion

Variable Items	Extent of (dis)agreement			Mean	Std. Devn
	Accepted	Neutral	Disagreed		
	f (%)	f (%)	f (%)		
There is existence of data from the embedded system used without clients' consent and knowledge.	70 (93.3%)	5 (6.7%)	0 (0.0%)	3.90	1.129
The data from the embedded systems are used without the client consent.	68 (90.6%)	5 (6.7)	2 (2.7%)	3.66	1.142
Consent from the client, will it enhance confidentiality and privacy.	65 (88.6%)	2 (2.7%)	8 (10.7%)	3.63	.982
Companies use endpoint protector to control and regulate the use of data in motion	64 (85.3%)	8 (10.7)	3 (4%)	3.34	1.235
Companies tend to use encrypting data on the devices to protect against data compromise and theft	59 (78.6%)	11 (14.7%)	5 (6.7%)	3.22	1.117
Performing strong identify verification ensure data in motion are not compromised	58 (77.3%)	10 (13.3%)	7 (9.4%)	3.58	.921
Companies enforce communication via secure channels enhance privacy and confidentiality of data in motion	57 (76%)	10 (13.3)	8 (10.7%)	3.48	1.165

Source: Primary data, 2023

6.2 Enhancing the Confidentiality and Privacy of Data in Motion

The study found out FMS Clients opinion on the enhancing the confidentiality and privacy of data in motion. Table 4.4 provide in summary of their views in frequency and percentages.

Table 6.3: Descriptive Results on Enhancing the confidentiality and privacy of data in motion

Variable Items	Extent of (dis)agreement			Mean	Std. Dev
	Accepted	Neutral	Disagreed		
	f %)	f (%)	f (%)		
Confidentiality and privacy is key in information security	69 (92%)	4 (5.3%)	2 (2.7%)	3.91	.957
Enhancing confidentiality and privacy of data in motion in embedded systems save losses financially.	67 (89.3%)	5 (6.7)	3 (4%)	3.62	1.011

Information from embedded systems is not fully safe.	65 (86.6%)	2 (2.7%)	8 (10.7%)	3.51	.943
The consent from end users can minimize unauthorized access to information	64 (85.3%)	8 (10.7%)	3 (4%)	3.23	.937
Confidentiality and privacy of data in motion can lead to avoidance of reputation risks as a result of data breaches	59 (78.6%)	11 (14.7%)	5 (6.7%)	3.63	982
Data privacy and confidentiality in motion can lead to avoidance of financial penalties as a result of data breaches	58 (76%)	10 (13.3%)	8 (10.7%)	.34	1.235
Secure environment minimized compromise of the integrity of data in motion in embedded systems	42 (56%)	12 (16%)	21 (28%)	3.22	1.117

Source: Primary data, 2023

6.4 The ECPDM Framework

The study aimed at designing a framework and its algorithms aimed at enhancing confidentiality and privacy of data in motion as illustrated in Figure 5.2 below:

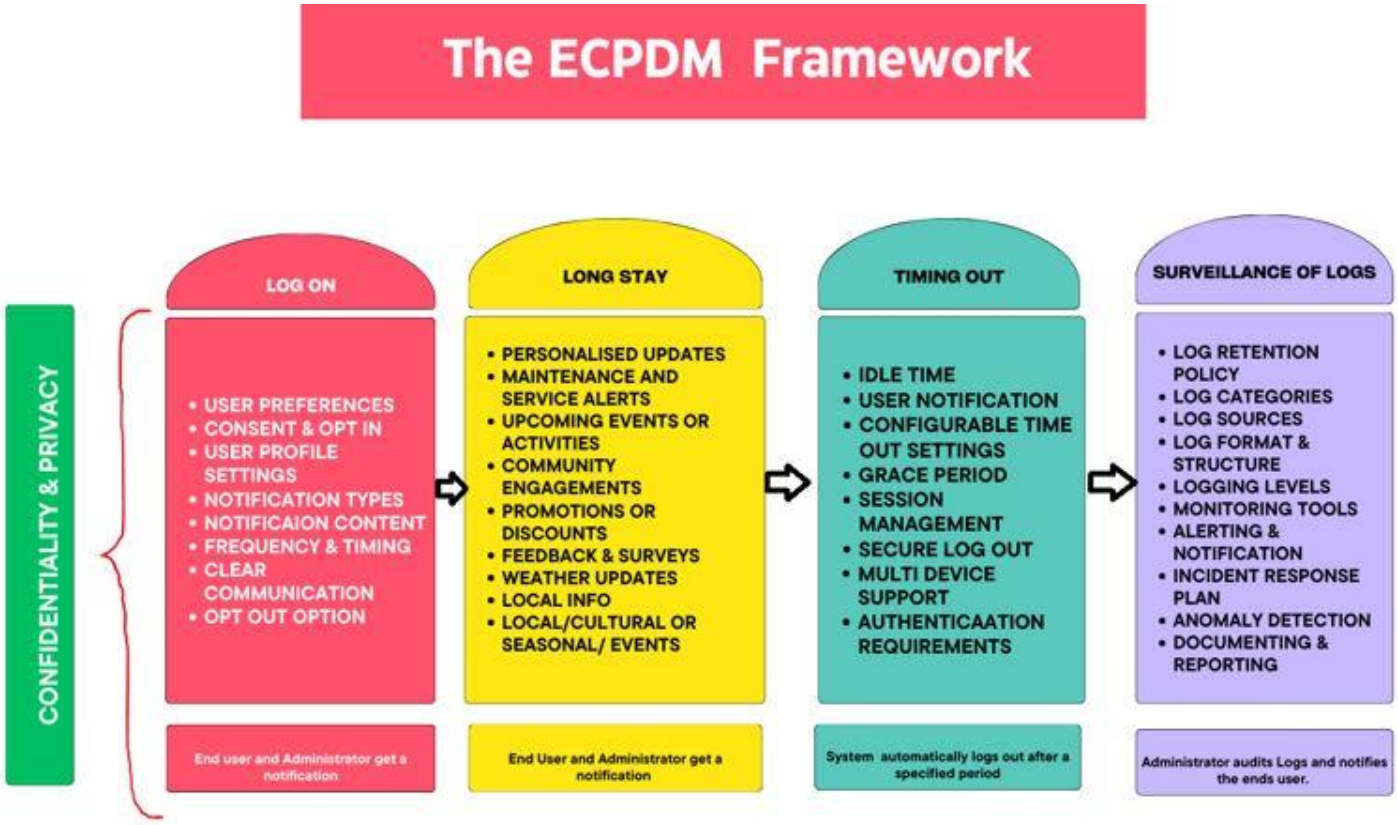


Figure 6.2: The ECPDM Framework
Source: Primary data, 2023

The described framework in figure 5.2 above was designed to enhance the confidentiality and privacy of data in motion through a specific mode of operation that involves user logon, automated notifications, session timeouts, and surveillance logs. The primary aim of this framework is to ensure that sensitive data remains protected while it is being transmitted or accessed within a system.

6.5 Data Flow of the ECPDM Framework

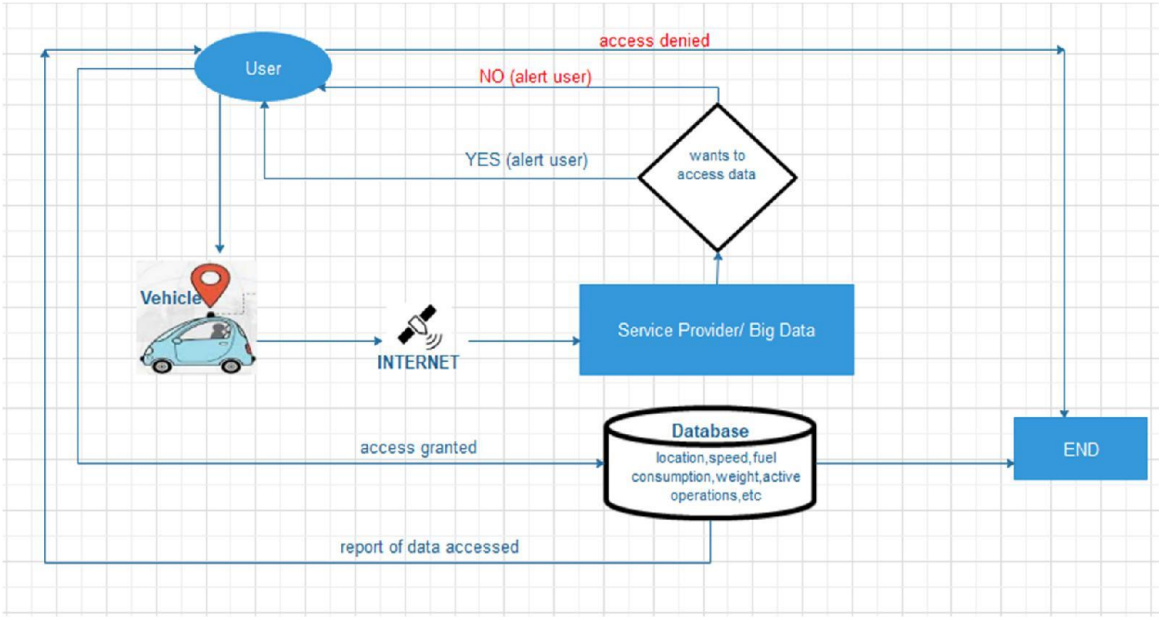


Figure 6.3: Showing data flow in the designed modified framework

The above illustration shows that data is transmitted from the sensors embedded in the vehicle and later forwarded to the internet, and this is done through the IoT gate-way. The user is notified if any one attempt to access his/her data (vehicle data) at this point the user can allow or deny access. Interestingly, this form of algorithm and framework empowers the end-users to have the final decision on who retrieves the available data. This is contrary to the period before when the service provider could access the data with or without seeking consent from the customer. Hence, this study aims at effectively monitoring the usage of client-data by the significant service providers, and the User is aware of who has accessed the data as well as at what time and can deny access thus enhancing confidentiality and privacy of data.

6.6 Use Case of the ECPDM Framework

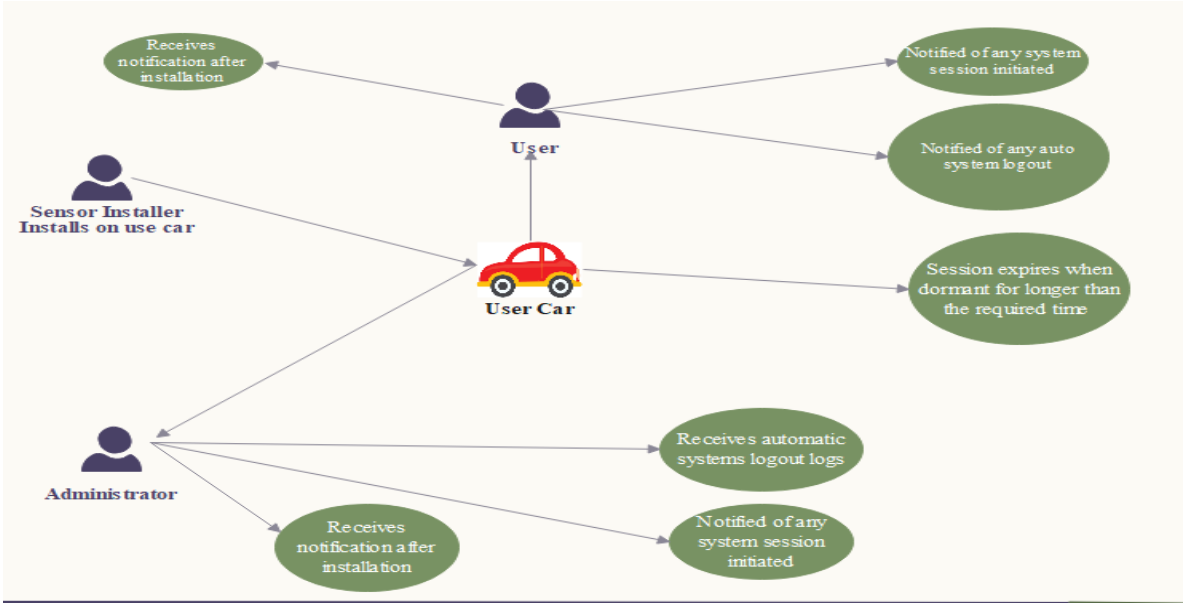


Figure 6.4: Showing Mode of Operation for a Use Case for a Framework and Algorithms

6.7 Description of the ECPDM Framework

Mode of operation of the framework and the algorithms involved:

End User: The process begins with the systems being installed in the end user car by the sensor installers. This step involves the installers accessing the end user car, and

installing the system. Proper authentication mechanisms are likely in place to verify the user's identity and eventual access to the system.

Administrator Notification: Once the system is successfully installed on the end user car, the system triggers a notification to the administrator and the end user. This notification serves as an alert that a user has been added on to the system. This initial notification is important for maintaining awareness of user installation and registration.

Session Monitoring: The framework continuously monitors system session duration whenever an administrator or any authorized person is logon. If the administrator remains logged on for an extended period of time (beyond what is recommended by the system), the system triggers another notification to the end user and administrator. The system also triggers a notification to the end user for any session initiated on the system. This notification is meant to alert the end user and flag prolonged sessions, which might indicate suspicious or unauthorized activity.

Log On: To ensure that end users receive notifications upon logging in, you'll need to implement a notification system within your platform. Here are some

End User Notification: After the automated logout, the administrator reviews the surveillance logs to assess the activities during their session. If any suspicious or unauthorized actions are detected, the administrator notifies the end user about these findings. This step serves as a deterrent against malicious activities and helps maintain transparency regarding user actions.

7.0 EVALUATION RESULTS

The correlation analysis was undertaken to examine the strength and direction of the relationships between the independent and dependent variables as explained in the Table below.

Table 7.1: Correlation analysis

Correlations		
		Effectiveness of the designed framework of data in motion
Consent	Pearson Correlation	.686 **
	Sig. (1-tailed)	.000
	N	44
		Effectiveness of the designed framework of data in motion
Confidentiality	Pearson Correlation	.342**
	Sig. (1-tailed)	.002
	N	44
		Effectiveness of the designed framework of data in motion
Privacy	Pearson Correlation	.589 **
	Sig. (1-tailed)	.000
	N	44

**. Correlation is significant at the 0.01 level (2-tailed).

Results in the Table 6.1 above reveal a significant relationship between consent and the effectiveness of the designed framework of data in motion. The correlation coefficient of .686 (**) with a significance value of .000 explain the nature of the relationship in this situation. This implies that seeking consent enhance trust and honesty, and empower the users to have the final say on who retrieves their data unlike before when the service provider and other third parties would without seeking permission from the client.

Multiple regression analysis was used to compute the variation shared by the variables. It was used to identify how much variation lies in the relationship between the efficiency and the designed framework of data in motion, as presented in Table 6.2 and Table 6.3.

Table 7.2: Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.713a	.508	.488	.71577679

a. Predictors: (Constant), Consent, Confidentiality and Privacy

Source: Primary data, 2023

From the model summary in Table 6.2, the multiple regression coefficient R was evidenced by 0.713. However, the adjusted R2 shows that the ethical issues accounts for 50.8% of the efficiency of designed framework of data in motion; implying that the efficiency of designed framework of data in motion can be explained by 50.8% of their ethical issues; and the remaining 49.2% variation in the efficiency of designed framework of data in motion is due to other factors that were not part of this study.

Table 7.3: Coefficients table

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	3.913	.129		.000	.000
	Consent	.245	.137	.245	1.783	.001
	Confidentiality	.304	.137	.304	2.220	.031
	Privacy	.313	.137	.313	2.310	.042

a. Dependent Variable: Performance of LTIL

Source: Primary data, 2023

The coefficients table 6.3 shows that specifically, consent accounts for 24.5% variation in the efficiency of designed framework of data in motion. Further, confidentiality accounts for 30.4% variation in the efficiency of designed framework of data in motion. Furthermore, privacy accounts for 31.3% variation in the efficiency of designed framework of data in motion. The findings revealed that confidentiality and privacy had the highest effect on the efficiency of designed framework of data in motion.

Table 7.4: Experts' Results

Statement	Mean	Std. Deviation	Interpretation
Data from the embedded systems is used with clients' consent and knowledge.	4.15	1.12	Agree
The client authorizes who accesses his/her data and when.	4.21	1.15	Agree
Consent from the client, enhanced confidentiality and privacy.	4.32	1.26	Strongly agree
Providing a notification to the user/client when there is attempt to access his/her data ensures data in motion is not compromised or misused	4.24	1.12	Agree
The ECPDM framework is effective	4.16	1.28	Agree
The ECPDM framework is efficient	4.35	1.35	Strongly Agree
The ECPDM framework is reliable	4.20	1.11	Agree
There is existence of data from the embedded system used without clients' consent and knowledge.	2.00	1.10	Disagree
Aggregate Mean	3.95	1.18	

According to the results in the table above, the study respondents generally agreed that the framework is largely effective and efficient in enhancing confidentiality and privacy of data in motion as evidenced by a mean score of 3.95 plus a standard deviation of 1.18 from Experts' results as shown.

8.0 CONCLUSIONS AND RECOMMENDATIONS

8.1 Conclusions

The study summarized that while data in motion and data at rest have different vulnerabilities and attack vectors, there are many software solutions that can help protect both. Antivirus, firewalls software, Data Loss Prevention (DLP) solutions, and encryption all contribute to the protection of data in motion and at rest. Data security has many overlaps with data privacy. The same mechanisms used to ensure data privacy are also part of an organization's data security strategy. Therefore, organizations should have good governance, risk and compliance to help improve on data privacy and confidentiality. Governance creates controls and policies enforced throughout an organization to ensure compliance and data protection. Risk also involves assessing potential cyber-security threats and ensuring the organization is prepared for them; as well as compliance ensures organizational practices are in line with regulatory and industrial standards when processing, accessing, and using data. In an organization environment, cloud security should be a critical part of the organization's security strategy. An effective strategy involves protecting cloud infrastructure, cloud workloads, and the data itself.

It was concluded that there is existence of data from the embedded system used without clients' consent and knowledge. The data from the embedded systems are used without the client consent. Consent from the client, enhanced confidentiality and privacy. Companies tend to use endpoint protector, encrypting data, and identity verification to control and regulate the use of data in motion although it's not sufficient. It is also concluded that enhancing confidentiality and privacy of data in motion in embedded systems saves losses financially. Information from embedded systems is not fully safe, and the consent from end users only minimized unauthorized access and misuse of information. Confidentiality and privacy of data in motion would lead to avoidance of reputation risks as a result of data breaches. Lastly, it was concluded that deficiency of awareness from the end users, the presence of cyber threats, attacks and or breaches observed among data in motion, gaps in the existing data frameworks, human errors, limited knowledge and access to existing data frameworks, insecure file sharing and existence of malicious actions or third-party infiltrating data in motion; these are the major weaknesses in the existing framework.

8.2 Recommendations

The study recommended that organizations should perform security audits at-least every few months. This identifies gaps and vulnerabilities across the organizations' security posture.

The study recommended the need for defined security framework for data. There is need for building a data security plan, and this plan includes defining requirements that shall help safeguard data in motion, address possible situations that could result in breaches, and raise awareness among workers and partners. All the organization employees should be aware of the security risks that could expose the organization to fines and fees due to inadequate cyber-security procedures.

The study recommended the need for identifying critical assets and vulnerabilities. Thus, organizations should adopt a proactive security approach that includes classifying and categorizing data coupled with content, user, and context aware security protocols to protect their sensitive data effectively in every country. Organizations should also conduct risk assessments to discover the volume of sensitive data they hold, how it moves, liability costs, and the number of users who have access to sensitive data.

The study recommended the need to implement technologies and processes. Thus, implementing systems and processes that ensure the safe transfer of sensitive data is vital towards ensuring data leaks and data theft are minimized. Data encryption plays a vital role in this step, and organizations should integrate it into common business workflows. Encryption requirements should be based on the latest standards by only allowing secure protocols.

It is also recommended that organizations looking into safeguarding data in transit against inside or outside attackers like malware attacks or intrusions should implement network security solutions such as firewalls and network access controls. Data Loss Prevention (DLP) solutions usually address the threats data in motion faces from breaches and human error during its transit.

The study recommended that encryption is another pertinent measure used to secure data both at rest and in motion. Encrypting hard drives using operating systems' native data encryption solutions, organizations can ensure that, if a device lands in the wrong hands, no one can access the data on the hard drive without an encryption key.

The study recommended the need for password hygiene, which is one of the simplest best practices for data security to ensure users have unique and strong passwords. Without central management and enforcement, many users shall use easily guessable passwords or use the same password for many different services.

The study recommended the need for authentication and authorization. Organizations must put in place strong authentication methods, such as OAuth for web-based systems. It's highly recommended to enforce multi-factor authentication when any user, whether external or internal, requests sensitive or personal data. Additionally, organizations must have a clear authorization framework in place, which ensures that each user has exactly the access rights they deserve to perform a function or consume a service, and no more.

REFERENCES

1. Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. Sensors, 22(5), 1969.

2. Abdiakhmetova, Z., Temirbekova, Z., & Turken, G. (2023). Intelligent Monitoring System Based on ATmega Microcontrollers in Healthcare with Stress Reduce Effect. In Computational Methods in Psychiatry (pp. 51-71). Singapore: Springer Nature Singapore.
3. Adler, P., & Florida, R. (2021). The rise of urban tech: how innovations for cities come from cities. Regional Studies, 55(10-11), 1787-1800.
4. African Union (2020). The Digital Transformation Strategy for Africa (2020-30).
5. Aggrey, O., & Evarist, N. (2019). Survey of Crowd Detection Algorithms using Wireless Sensor Networks: A Case of People Crowds. Article in International Journal of Computer Applications, 182(38), 975–8887. https://doi.org/10.5120/ijca2019918383
6. Agrawal, S., Schuster, A. M., Britt, N., Mack, E. A., Tidwell, M. L., & Cotten, S. R. (2023). Building on the past to help prepare the workforce for the future with automated vehicles: A systematic review of automated passenger vehicle deployment timelines. Technology in Society, 72, 102186.
7. Abaho, E. (2017). *Advancing Transportation in Uganda with Automation, Connectivity and Intelligence.* Kampala: MUK (Dissertation)
8. William, A., Mirembe (PhD), D. D. P., & Nabaasa (PhD), D. E. (2022). Data Privacy Analysis on E-commerce Application. *International Journal of Technology and Management*, *7*(2), 1-29. Retrieved from https://www.utamu.ac.ug/ijotm/index.php/ijotm/article/view/105
9. Barecki, B. (2019). *How to Protect Data in Motion.* Confidentiality and Privacy of Data. 3rd edition. Los Angeles, Sage.
10. Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/J.JACCPUBPOL.2018.10.006
11. William, A., Mirembe (PhD), D., & Nabaasa (PhD), E. (2023). Reducing Misuse of Data in Motion through Surveillance of Logs. *International Journal of Technology and Management*, *8*(1), 1-10. Retrieved from http://utamu.ac.ug/ijotm/index.php/ijotm/article/view/108
12. Haber, M. J., & Rolls, D. (2020). Identity Attack Vectors. In *Identity Attack Vectors* (pp. 107–116). Apress. https://doi.or/978-1-4842-5165-2_10*Hadoop*. (n.d.).
13. Katushabe, B.W. (2021). *Benefits of GPS Tracking Devices for Personal Vehicles*. Kampala. (KIU Dissertation). Unpublished.
14. Kagita, M. K., Thilakarathne, N., Rajput, D. S., & Lanka, D. S. (2020). *A Detail Study of Security and Privacy issues of Internet of Things*. http://arxiv.org/abs/2009.06341
15. Krejcie, R.V. & Morgan, D.W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement.*
16. Lu, Y., & Xu, L. Da. (2019). Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847
17. Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). Secure data transmission through reliable vehicles in vanet using optimal lightweight cryptography. In *Advanced Sciences and Technologies for Security Applications*. Springer. https://doi.org/10.1007/978-3-030-16837-7_9
18. Mukasa, D. (2021). *A GPS Tracker on Every 'Boda Boda':* A Tale of Mass Surveillance in Uganda. Kampala. Unwanted Witnesses.
19. Oppitz, M., & Tomsu, P. (2018). Security and Privacy Challenges. In *Inventing the Cloud Century* (Vol. 6, Issue 1, pp. 377–410). https://doi.org/10.1007/978-3-319-61161-7_14
20. Wlosinski, L. G. (2018). Data Loss Prevention — Next Steps. *ISACA Journal*, *1*, 1–11. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-1/data-loss-prevention-next-steps_joa_eng_0218