December 31, 2024 Vol. 6 No. 9 E-ISSN 3027-0952 P-ISSN 3027-2033

International Journal of

CONVERGENT AND INFORMATICS SCIENCE RESEARCH (IJCISR)

www.harvardpublications.com

DEVELOPMENT AND DEPLOYMENT OF A SECURITY INFORMATION MANAGEMENT SYSTEM FOR ENHANCED ORGANIZATIONAL SAFETY AND EFFICIENCY

AMANNAH, CONSTANCE IZUCHUKWU
Department of Computer Science, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria.
Corresponding Author: *aftermymsc@gmail.com*

DOI: https://doi.org/10.70382/hijcisr.v06i9.002

Abstract

The study focuses on the development and deployment of a Security Information Management System (SIMS) to enhance organizational safety and efficiency. It addresses the critical need for robust data security frameworks in modern organizations, emphasizing the protection of information integrity, availability, and confidentiality. Rooted in historical and evolving security paradigms, the research highlights the transition from traditional military-focused strategies to comprehensive approaches encompassing economic, environmental,

Keywords: Deployment, Security, Information Management Sytemen, Organizational Safety, Development.

INTRODUCTION

Data frameworks are critical to the functioning of modern organizations, as they house the essential information and resources needed to support business operations. Ensuring the security of these systems is paramount, as it guarantees data integrity, availability, and reliability for timely usage. In the context of national security, protecting sensitive data goes beyond safeguarding information; it encompasses strategic elements such as financial resources, trained personnel, and logistical capabilities. Historically, significant advancements in security practices followed World War II, with initial emphasis on military and police operations. Over time, the scope of security has expanded to include economic, environmental, and energy dimensions, reflecting the interconnected and multifaceted nature of contemporary security concerns.

and technological dimensions. Using the Object-Oriented System Development Methodology (OOSDM), the study designed and implemented a real-time SIMS integrating authentication and authorization processes. The proposed system features modular architecture comprising Web, Application, and Data tiers to ensure scalability, security, and efficiency. Advanced tools, such as encryption, intrusion detection systems, and login tracking, safeguard against cyber threats, including hacking and denial-of-service attacks. Rigorous testing of the system demonstrated its effectiveness in mitigating security risks, supporting decision-making with timely data access, and enhancing operational efficiency. The findings underscore the potential of SIMS to secure sensitive organizational data and recommend its adoption, training for security personnel, and regular updates for sustained functionality. This research contributes to advancing information security practices, particularly in dynamic operational environments.

Security is a complex and context-dependent concept, interpreted differently by various stakeholders, including researchers, policymakers, and organizations. Barry Buzan (1991) aptly described security as an ambiguous and multi-dimensional idea, often dominated by military perspectives. At its core, security fosters peace, stability, and protection of resources, enabling societal growth and resilience. Over the decades, the understanding of security has evolved, incorporating psychological, economic, informational, and technological dimensions.

In today's digital era, information security has emerged as a critical concern, particularly for organizations and military operations that rely on data as a strategic asset. The interplay of technology, users, and business processes shapes the vulnerabilities of information systems, necessitating robust measures to safeguard privacy, accessibility, and integrity (Posthumus et al., 2007). Cyberattacks such as those targeting Estonia in 2007 and Georgia in 2008 demonstrate the significant impact of information warfare (Tikk, 2008; Tikk et al., 2008). The rise of cyber threats, including malware, denial of service attacks, and social engineering techniques, highlights the need for advanced strategies to counteract such risks (Kurose & Ross, 2010; Hadnagy et al., 2011). Military organizations, in particular, face heightened risks due to the strategic value of information in achieving objectives like information dominance and information warfare (Alberts et al., 2001). The reliance on information technology as both a tool and a target necessitates innovative approaches to information security planning, with a focus on preempting adversarial strategies. This study aims to address these challenges by developing and deploying a Security Information Management System (SIMS) that enhances organizational safety and efficiency. Through this effort, the research seeks to establish a robust framework for safeguarding critical data and mitigating security risks in dynamic operational environments.

By examining existing vulnerabilities and integrating cutting-edge security practices, this study contributes to a deeper understanding of information security and its application in various organizational contexts, including military, governmental, and civilian domains.

Related Literature

a. Theoretical Review

A theoretical framework provides a foundational structure of existing theories that guides the development of arguments and supports the purpose of a study.

Protection Motivation Theory (PMT), proposed by Rogers (1975), explains how individuals protect themselves by assessing two key factors: the perceived threat and their coping mechanisms. Threat appraisal involves evaluating the severity and relevance of a situation, while coping appraisal examines an individual's ability to manage the situation. Threat appraisal consists of perceived severity and perceived vulnerability, while coping appraisal comprises perceived self-efficacy and perceived response efficacy. Perceived response efficacy refers to the belief that the proposed action will mitigate the threat, and perceived self-efficacy is the belief in one's ability to perform the recommended actions.

PMT has been applied in the context of information security to understand user behavior. For instance, Anderson and Agarwal (2010) used PMT to study the psychological, social, and cognitive factors influencing individuals' decisions to perform security-related tasks. They found that factors such as organizational commitment, resource availability, and perceived self-efficacy impact users' intentions to adhere to security policies. PMT has also been extended by the Technology Threat Avoidance Theory (TTAT), which posits that individuals are motivated to adopt safety measures only when they cannot avoid perceived risks (Agarwal & Anderson, 2010). This framework underlines the importance of innovative technological security systems to enhance information protection.

The Cyber Attack Theory, discussed by Zhuang (2014), emphasizes that an attacker's success is contingent on the information available during an attack. The theory highlights the centrality of information in cyberattacks, describing how attackers aim to access or manipulate critical system parameters, termed "information boundaries." These boundaries encompass configuration parameters, execution states, and system data, all of which are potential targets for exploitation.

Zhuang (2014) further introduces the concept of a "data boundary," a comprehensive set of parameters defining a system. Attackers seek to exploit these boundaries to gain control or disrupt operations. This perspective provides a framework for studying how attackers interact with Moving Target Defense (MTD) systems, emphasizing the dynamic interplay between attack strategies and defense mechanisms. Understanding these interactions is crucial for designing robust security frameworks that can mitigate evolving cyber threats effectively. Impression Management Theory (IMT), introduced by Goffman (1959), explores how individuals consciously or unconsciously manage information to influence others' perceptions. IMT suggests that individuals strategically control their actions and presentations to achieve specific goals (Bozeman & Kacmar, 1997). This theory has been widely applied in sociology, psychology, management, and education to understand social behavior.

Leary and Kowalski (1990) identified two key processes in IMT: **impression construction** and **impression motivation**. Impression construction involves the deliberate crafting of one's image, while impression motivation reflects the desire to achieve specific social or personal objectives. IMT has gained prominence in online interactions, where actions and statements can significantly impact perception in digital spaces (Guadagno & Cialdini, 2007). For example, men tend to employ assertive tactics, while women prefer cooperative strategies (Guadagno & Cialdini, 2007). In the context of information systems, IMT is critical for understanding user behavior and organizational dynamics. The advent of ICT and user-generated content on platforms like Web 2.0 amplifies the influence of online impression management. Tedeschi and Rosenfeld (1981) noted that individuals often seek consistency in external perceptions to facilitate smoother social interactions. IMT has laid the groundwork for examining the psychological underpinnings of behavior in both individual and organizational settings, highlighting its relevance in designing secure and user-oriented systems.

These theoretical perspectives- PMT, Cyber Attack Theory, and IMT- form the basis for understanding the multifaceted challenges of information security. PMT provides insights into user motivation and behavior, Cyber Attack Theory focuses on the strategies and dynamics of cyber threats, and IMT emphasizes the role of perception and behavior in social and organizational contexts. Together, they underpin the design and implementation of effective security information management systems.

b. Conceptual Framework

Security is a multifaceted and essential concept that carries different meanings for various groups, including researchers, policymakers, and organizations. At its core, security encompasses peace, safety, stability, and the protection of human and physical resources, ensuring the absence of crises or threats to fundamental rights. This foundational perspective aids societal growth and progress (Buzan, 1991). Historically, security's scope has expanded beyond traditional military concerns to include economic, environmental, and social dimensions. Barry Buzan (1991) describes security as a broad, ambiguous concept that primarily focuses on preventing harm and preserving a state's identity and functionality against hostile forces. Similarly, Bodunde et al. (2014) highlight that security involves safeguarding individuals and assets from harm, fear, and threats, while William (2008) associates it with mitigating risks to critical values. Ogaba (2010) further defines security as the absence of threats that could undermine a nation's development, values, and the well-being of its citizens.

The traditional security paradigm, rooted in Cold War-era thinking, prioritizes military strength and deterrence strategies (Walt, 1991). However, critiques like Buzan (1991) argue for an expanded view that includes non-military threats such as economic instability, environmental degradation, and social inequities (Ochoche, 1997). This modern perspective, endorsed by scholars like Ogunsanwo (1997), advocates for a broader understanding of security, emphasizing the well-being of individuals and communities. The concept of human security shifts focus from state-centric to people-centric approaches, aiming to protect individuals from both traditional and non-traditional threats. According to the Commission on Human Security (CHS), human security is "the protection of the vital core of all human lives in ways that enhance human freedoms and human fulfillment" (Adedoyin, 2013). Hubert (1999) underscores its importance in safeguarding individuals from both violent and non-violent threats, ensuring their rights and dignity.

Human security comprises seven dimensions:

i. **Economic security:** Steady income and protection from poverty and unemployment.
ii. **Food security:** Consistent access to sufficient and nutritious food.
iii. **Health security:** Protection from diseases, malnutrition, and lack of healthcare.
iv. **Environmental security:** Safety from natural disasters and environmental degradation.
v. **Personal security:** Protection from violence, including domestic abuse and ethnic conflicts.
vi. **Community security:** Safeguarding traditional values and relationships from internal and external threats.
vii. **Political security:** Ensuring fundamental human rights and protection from political repression (UNDP, 1994).

National security refers to a state's ability to protect its territory, resources, and citizens from internal and external threats. Traditional definitions focus on military power and territorial integrity (Lippmann, 1944; Maniruzzaman, 1982). However, contemporary perspectives, as noted by McNamara and Nwolise (2008), emphasize addressing non-military challenges such as poverty, unemployment, and environmental degradation. Obasanjo (1999) broadens the scope of national security to encompass the security interests of all citizens, while Maier (2013) links it to domestic and international stability. International security focuses on cooperative efforts by nations, regional groups, and international organizations to maintain global stability. Buzan (2000) argues that it involves identifying and addressing threats that could disrupt international harmony. The UNDP (1994) emphasizes safeguarding populations from violent conflicts, poverty, and socio-political issues, framing international security as both a collective and individual responsibility.

Information security aims to protect data from unauthorized access, misuse, or destruction. The "onion model of defense" illustrates the layered approach to securing data, from encrypted networks to reliable host systems. Key principles—Confidentiality, Integrity, and Availability (C-I-A)- form the foundation of information security (Anderson, 2003). These principles ensure data is accessible, accurate, and protected from unauthorized use. Authentication systems safeguard user identities and system resources against threats. These systems are categorized as knowledge-based (e.g., passwords), token-based (e.g., RFID), or biometrics-based (e.g., fingerprints) (Allen & Bahr, 2014). Each method offers unique advantages and vulnerabilities, necessitating tailored security solutions for specific contexts.

Insurgents and organized armed groups pose significant security threats by challenging state authority and destabilizing societies. Insurgent groups often pursue political goals, leveraging violence to undermine governments (O’Neill, 1990). Organized criminal groups, in contrast, primarily seek financial gain through illegal activities like trafficking and smuggling, often using violence strategically to protect their operations (Schneckener, 2006). The proliferation of armed groups exacerbates security risks for states and individuals. Violent activities such as ethnic conflicts, terrorism, and organized crime destabilize societies, disrupt governance, and endanger lives (Alimba, 2014). Effective countermeasures require comprehensive strategies addressing both the root causes and immediate threats posed by these groups.

This conceptual framework establishes a comprehensive understanding of security, encompassing its traditional, human, national, and international dimensions, while highlighting specific challenges in information security, authentication, and the dynamics of armed groups. These insights form the foundation for developing and implementing robust security systems tailored to contemporary threats.

Methodology

This research adopted the **Object-Oriented System Development Methodology (OOSDM)** for designing, modeling, and implementing the proposed system. OOSDM treats the system as a collection of interacting classes and objects, allowing for a modular and intuitive representation of the system's functionality and structure.

The methodology was chosen for its numerous advantages:

i. **Effectiveness:** OOSDM enables a clear understanding of the system by focusing on real-world entities and their interactions, ensuring that the design aligns with user needs.

ii. **Efficiency:** The modular nature of object-oriented systems promotes streamlined development and easier debugging.

iii. **Reliability:** Encapsulation, inheritance, and polymorphism enhance system stability and adaptability by reducing code redundancy and ensuring consistency.

iv. **Reusability:** Classes and objects created during development can be reused in future projects, saving time and resources.

v. **Faster Development:** By leveraging pre-defined libraries and reusable components, OOSDM accelerates the system development process.

The adoption of OOSDM ensures that the system is robust, scalable, and aligned with best practices in software development, meeting both functional and non-functional requirements effectively. The methodology involves a systematic approach divided into clearly defined stages. Each stage ensures the system’s design, implementation, and deployment aligns with the goal of enhancing organizational safety and efficiency.

Current Security Information Management System

The current security information management system is partially digitized, relying on computer-based data storage and retrieval processes as shown in figure 1. However, the system is not designed to function in real-time. Data and information are recorded and stored on a computer but are only accessed or retrieved periodically or as needed, often after a certain time frame or approval process. This delayed access to operational data limits the system's effectiveness. One significant drawback of the existing system is its inability to process and analyze information in real time. This limitation leads to slower decision-making processes, as stakeholders lack immediate access to up-to-date information. The absence of real-time capabilities hampers the speed and accuracy of response actions, reducing operational efficiency. This analysis emphasizes the necessity of transitioning to a modern, real-time system that can ensure prompt decision-making and enhance operational effectiveness.

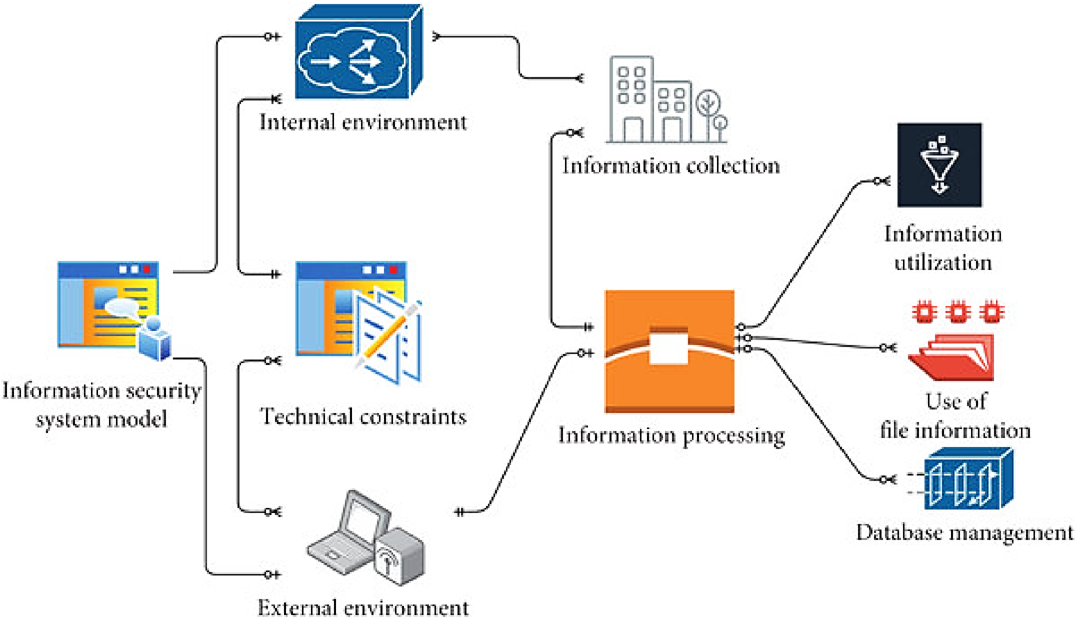

Figure 1 Architecture of the Existing System (Source: Shultz et al., 2004).

The Security Information Management System for Enhanced Safety and Efficiency

The proposed method operates in real time, leveraging computer systems to create, store, and retrieve security information efficiently. It incorporates a two-step security process: **authentication** and **authorization**, both critical for ensuring robust access control and system integrity. Authentication is the process of verifying a user's identity. It requires the user to provide credentials, such as a user ID and password, to confirm they are who they claim to be. By using reliable authentication mechanisms, the system ensures only legitimate users gain access to resources.

Once a user's identity is authenticated, the system implements authorization to determine their level of access. Authorization defines:

i. **Accessible resources:** Specifies the applications and modules the user can interact with.
ii. **Permitted actions:** Determines what tasks the user can perform (e.g., viewing, modifying, or deleting data).
iii. **Data accessibility:** Controls the type and scope of data users can handle.

Authorization is based on the user’s membership in one or more protection groups, which grant specific permissions. Authentication is set up in the **Security Groups app**, ensuring users are validated through their user ID and password. This process secures user identity before granting system access. Permissions are managed systematically for security groups, enabling efficient control over user rights. Each user has a **security**

profile, which is a collection of rights derived from their associated security groups. These profiles govern the tasks users can perform within the asset management system applications. User security profiles can be reviewed and managed through the **Users app's Security.** By aggregating all security groups, the system generates a comprehensive **security profile** for users. This approach allows for granular control over user rights and ensures secure access across organizational applications. Login tracking provides an added layer of security by monitoring login attempts. The system can:

i. Set a maximum number of allowed login attempts.
ii. Track and record failed login attempts.
iii. Automatically block users after exceeding a predefined number of attempts.

To protect sensitive information such as passwords and personal data, the system employs encryption. Using **Crypto** and **CryptoX** data types with the **Java Cryptography Extension (JCE)** ensures data confidentiality and integrity.

The system is designed to withstand potential threats such as:

i. **Hacking:** Attacks on login, password recovery, or self-registration processes.
ii. **Denial-of-Service (DoS):** Attempts to overwhelm the system and disrupt services.
These risks are mitigated by configuring security settings and modifying system properties to enhance resilience.

This proposed method enhances the organization's security infrastructure by combining real-time capabilities with robust authentication and authorization mechanisms. It addresses critical vulnerabilities, such as unauthorized access and service disruptions, ensuring the confidentiality, integrity, and availability of security information. The design of the system is structured into three distinct layers, ensuring modularity, scalability, and robust functionality. These layers are the **Web Tier**, **Application Tier**, and **Data Tier.**

The web tier is the system's front-end layer that interfaces with end-users and facilitates data exchange over the internet. It comprises the following components:

i. **End-User (Client):** Represents the users interacting with the system through a web browser or other client interface.
ii. **Certificate Authority Authentication Identification (CA Auth ID):** Ensures secure identification and authentication of users, leveraging certificate-based mechanisms to validate identities.
iii. **Web Server:** Acts as the intermediary between clients and the application tier, handling HTTP requests and serving web content securely.

This tier enables seamless physical and logical data exchange between connected devices over the web. The application tier functions as the system's middle layer, hosting the core business logic and application services. Key components include:

i. **Administration Console:** Provides a graphical user interface (GUI) for managing applications, configuring system settings, and performing administrative tasks.
ii. **Application Server:** Executes business applications, processes user requests, and ensures secure communication using a defined protocol. It is built within a **WebSphere** environment, which supports application deployment, monitoring, and management.

This tier acts as a bridge, facilitating communication between the web and data tiers while delivering business functionalities. The data tier serves as the system's back-end layer, handling data storage, retrieval, and secure management. Its components include:

i. **User Repository:** Stores user credentials, profiles, and associated permissions.
ii. **System Database:** Maintains the core database for storing application data and logs.
iii. **User Data Service:** Manages user-specific data and interactions, ensuring secure and efficient access.
iv. **Strong Identification Server:** Provides advanced identity verification services to ensure secure access and operations.
v. **Hardware Security Module (HSM):** Safeguards sensitive cryptographic keys and performs secure cryptographic operations to protect data integrity and confidentiality.

This tier ensures the secure handling of all system data while supporting reliable operations across the entire architecture. The Design has the following Key Advantages;

1. **Modularity:** The separation into tiers allows for independent development, deployment, and management of each layer.
2. **Scalability:** Each tier can be scaled independently to accommodate increased user demand or data load.
3. **Security:** Robust security mechanisms, such as CA Auth ID and HSM, provide strong authentication, data protection, and encryption.
4. **Efficiency:** Streamlined communication between layers ensures smooth data flow and system performance.
5. **Manageability:** The administration console and WebSphere environment provide user-friendly tools for managing applications and system tasks.

This tiered design ensures a reliable, scalable, and secure system that meets the needs of both users and administrators effectively. Figure 2 highlights the features of the architecture. The new system is designed in five design phases; input design, process design, output design, database design and security design. The entire five design phases synchronizes with the system architecture, current security information management system

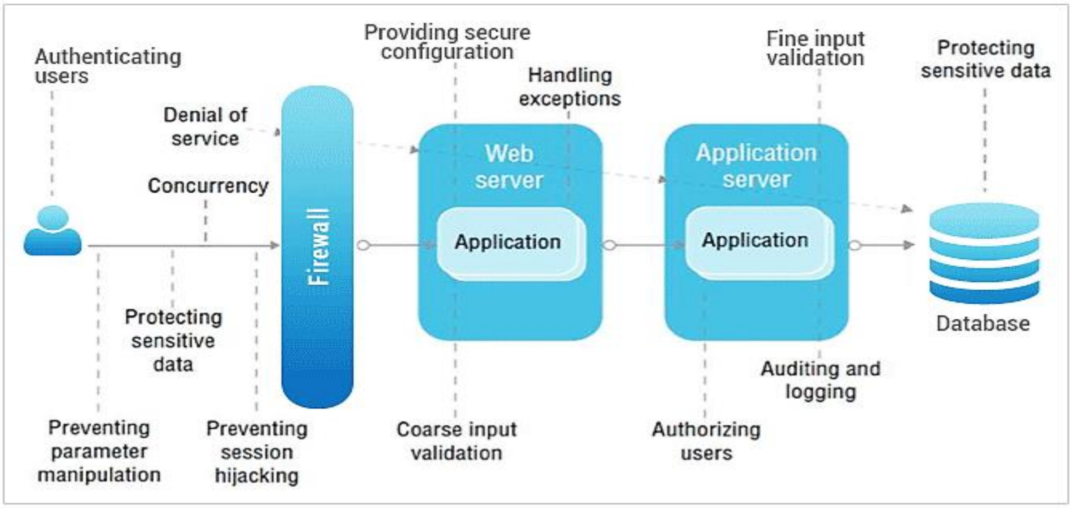

Figure 2 Architecture of the Security Information Management System for Enhanced Safety and Efficiency

The proposed method is computer-based, requiring users to provide information through various input devices as figure 3 illustrates. Inputs are critical for the system's functionality and efficiency, as they enable accurate user identification and access control. The system relies on the following user-provided information;

1. **Username and Password:** For initial authentication.
2. **Email Address:** Used for account creation, recovery, or notification purposes.
3. **Date and Time of Registration:** Records when the user accesses the system for accountability.
4. **Purpose of Use:** Logs the user’s intent to access specific system features or resources.

By capturing and processing this information, the system accurately identifies users and ensures secure and seamless operation. These inputs are fundamental for improving the system’s performance and maintaining high levels of security and user experience.

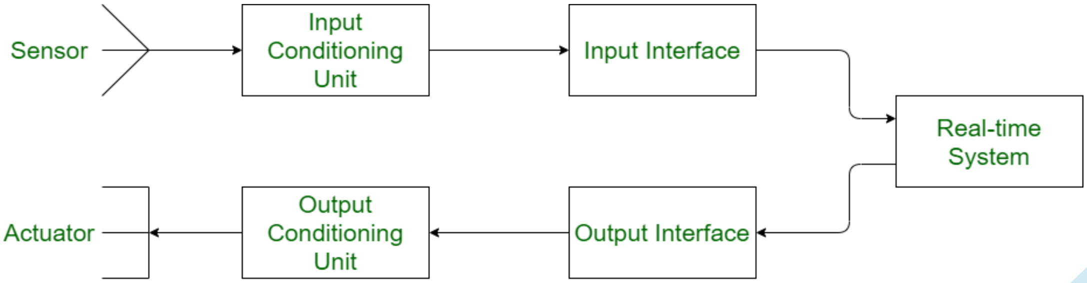

Figure 3 Input Design of the Proposed System

The **process design model** provides developers with all the graphical representations needed to understand and implement the suggested system's data flow and processes. This includes diagrams that visually depict the interactions between system components and actors, ensuring clarity and consistency during development. Before progressing to subsequent stages of development, the developer must conduct a **quality assurance (QA) check**. This involves reviewing completed steps to verify their correctness, validity, and adherence to system specifications. QA ensures that the process is built on a robust foundation, minimizing errors and discrepancies in later stages. The **Use Case Diagram** illustrates the interaction between various components and actors within the proposed system, specifically the **Issue Tracking System**. This diagram highlights the roles and responsibilities of the system's actors and the methods they use to interact with the system. Figures 4 to 5 show the USE-CASE, and Sequence diagrams.

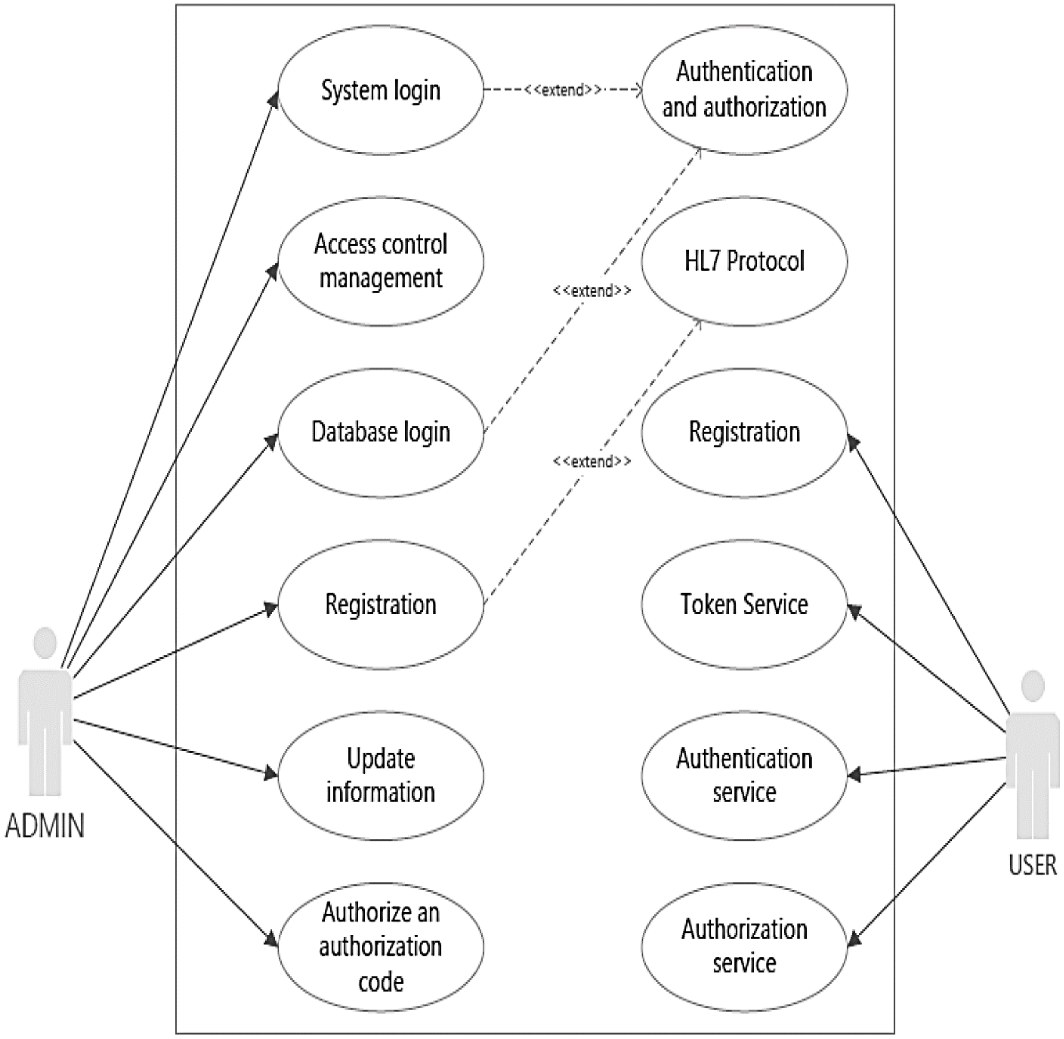

Figure 4 The process design using USE-CASE diagram

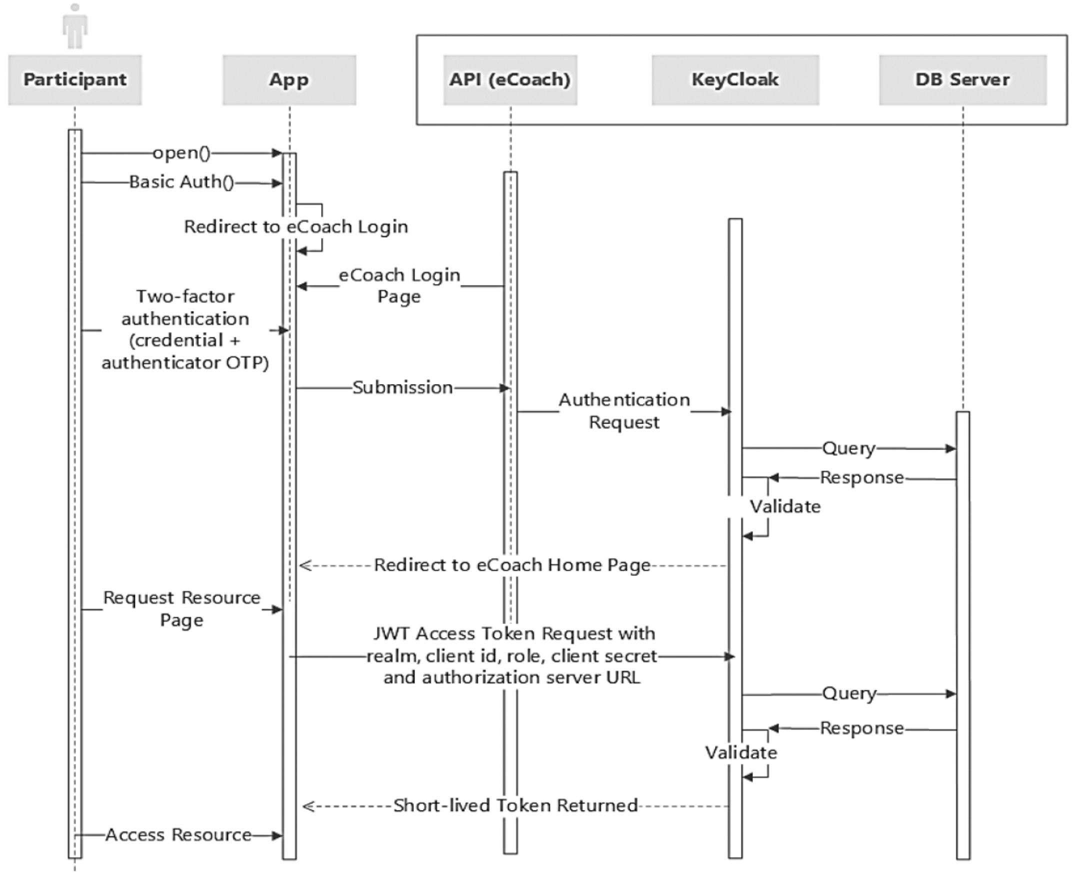

Figure 4 The process design using sequence diagram

The **MySQL Database System** was utilized to store and manage the system's information. Figures 6 to 7 illustrate the various database files schemas employed in implementing the system. The database design incorporates both **logical** and **physical models**, ensuring a structured and efficient approach to data management.

Logical Data Model:

i. Focuses on defining the data elements and their interrelationships.
ii. Helps in organizing the data conceptually, based on the system's requirements.
iii. Ensures clarity in the representation of entities, attributes, and relationships, which form the backbone of the database structure.

Physical Data Model:

i. Translates the logical data model into a real database implementation.
ii. Accounts for the system's technical requirements, such as storage, indexing, and performance optimization.
iii. Guides the creation of tables, columns, data types, and constraints in MySQL, aligning with the logical model.

The logical model ensures that the data structure aligns with the functional needs of the system, while the physical model focuses on the practical aspects of database implementation. Together, these models ensure a robust, scalable, and well-structured database design for efficient system operations.

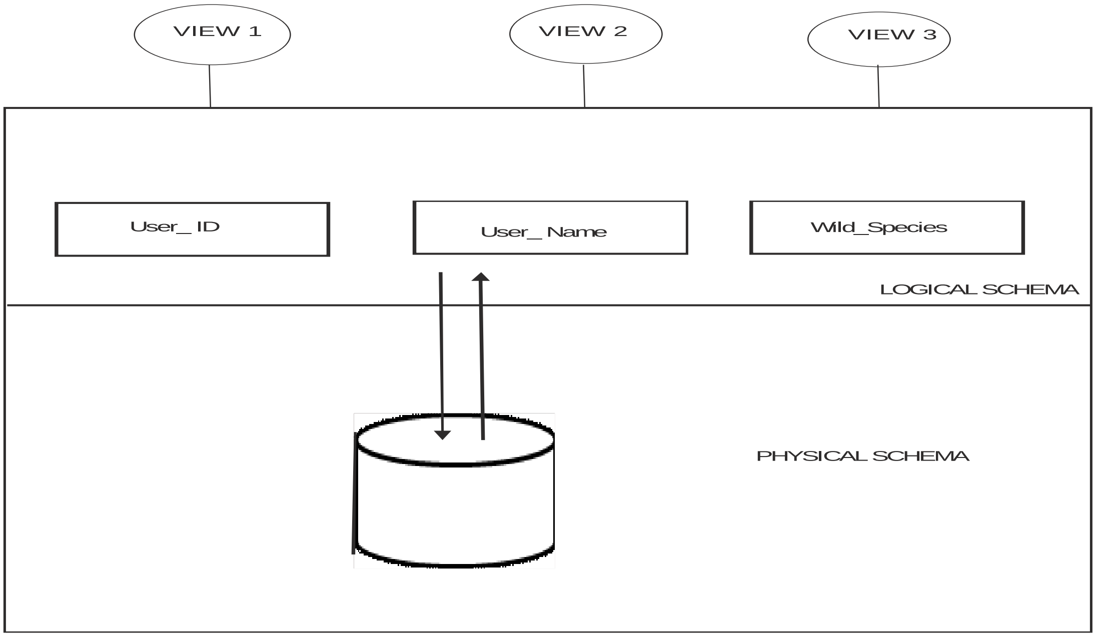

Figure 6 Logical schema of the system database

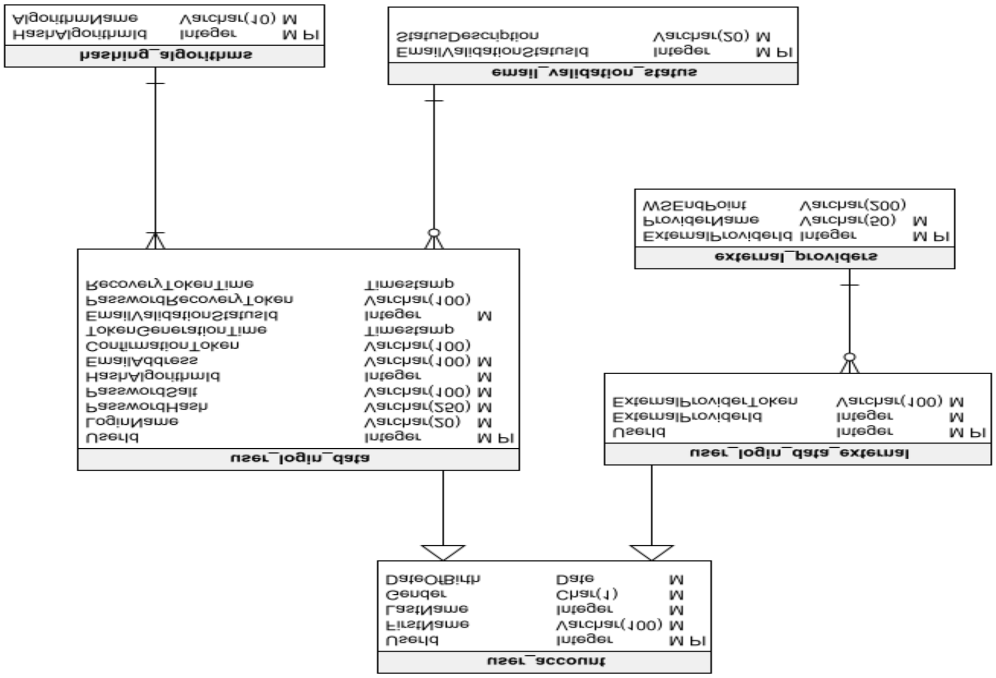
hashing_algorithms
HashAlgorithmId Integer M PI
AlgorithmName Varchar(10) M
email_validation_status
EmailValidationStatusId Integer M PI
StatusDescription Varchar(20) M
external_providers
ExternalProviderId Integer M PI
ProviderName Varchar(50) M
WSEndPoint Varchar(200)
user_login_data
UserId Integer M PI
LoginName Varchar(20) M
PasswordHash Varchar(250) M
PasswordSalt Varchar(100) M
HashAlgorithmId Integer M
EmailAddress Varchar(100) M
ConfirmationToken Varchar(100)
TokenGenerationTime Timestamp
EmailValidationStatusId Integer M
PasswordRecoveryToken Varchar(100)
RecoveryTokenTime Timestamp
user_login_data_external
UserId Integer M PI
ExternalProviderId Integer M
ExternalProviderToken Varchar(100) M
user_account
UserId Integer M PI
FirstName Varchar(100) M
LastName Integer M
Gender Char(1) M
DateOfBirth Date M

Figure 7 Logical schema of the system database

The framework, as a security information system, requires continuous monitoring and safeguarding to ensure its integrity and reliability. Various mechanisms and tools are integrated into the framework to maintain data security and system functionality.
The data integrity mechanism ensures that information remains accurate and consistent during transmission and storage. The process involves:

1. **Checksum Generation:** A value is created from the data itself through a specific algorithm.
2. **Transmission:** Both the data and the checksum are sent to the recipient.
3. **Validation:** The recipient generates a new checksum from the received data and compares it to the original checksum. If the two values match, the data integrity is confirmed.

This process ensures that the data has not been altered or corrupted during transmission. Figure 8 shows the security tools and technologies as shown below;

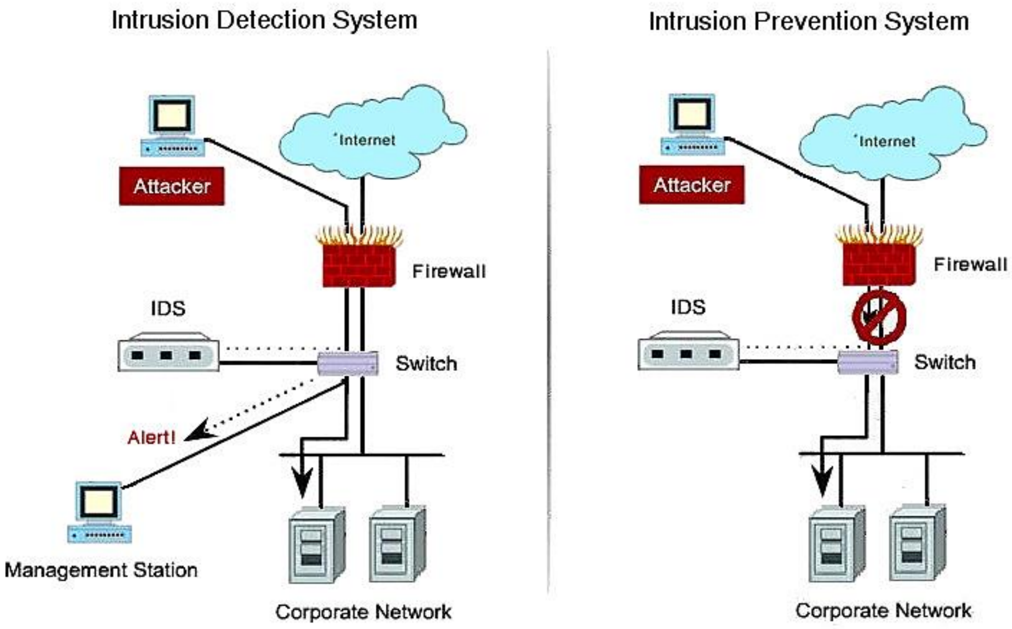

Figure 8 Security Mechanism of the Information Management System for Enhanced Safety and Efficiency

Intrusion Detection System (IDS): Monitors network traffic to detect unusual behavior. Sends alerts when potential threats are identified, enabling prompt response and mitigation.
Password Manager: Stores user credentials securely. Protects passwords in an encrypted format, ensuring they remain safe from unauthorized access.
Antivirus Software: Scans files in real time as they are created or accessed. Quickly identifies and neutralizes threats such as viruses and malicious code.
Encryption: Transforms data into ciphertext, making it unreadable to unauthorized users.Only authorized individuals with the correct decryption key can convert ciphertext

back to plaintext. Ensures confidentiality and prevents unauthorized access to sensitive information.

Results and Discussion

The study developed a comprehensive framework for a security information system. This model integrated essential components such as data collection, analysis, and reporting mechanisms, supported by protocols and procedures to ensure system effectiveness. The design process included; Identifying potential threats, conducting risk assessments, and defining countermeasures to address identified threats.

Following the design phase, the study implemented the security information model by; deploying necessary hardware, software, and infrastructure, configuring the system for seamless integration with existing security measures, and establishing guidelines for the system's use and maintenance to ensure operational efficiency.

The implemented system was subjected to rigorous testing to evaluate its performance in real-world scenarios. Key activities included; simulating various security situations to test threat detection and response, measuring the system’s ability to provide accurate, timely information for decision-making.

Summary and Conclusion

Summary

The increasing prevalence of data theft, unauthorized access, cyberattacks, and system vulnerabilities prompted this study to develop a secure information management framework. The study aimed to; design a security information model, implement the model, and test the model’s effectiveness in addressing security challenges. The **Object-Oriented System Development Methodology (OOSDM)** guided the work, with a use case diagram for system planning and Python as the primary development language. The proposed system successfully identified threats, raised security awareness, and established functional security information models.

Conclusion

The developed system incorporates core security services, ensuring robust protection of data and system resources:

i. **Authentication Service:** Verifies the claimed identity of users or systems.
ii. **Access Control Service:** Protects resources from unauthorized access.
iii. **Confidentiality Service:** Safeguards data against unauthorized disclosures.
iv. **Integrity Service:** Protects data from unauthorized modifications, insertions, or deletions.
v. **Non-Repudiation Service:** Ensures entities cannot deny prior actions or commitments.

Recommendations

To maximize the potential of the proposed system, the study recommends the following:

1. **Adoption by Security Agencies:** Security agencies should adopt the system and test its functionality in various operational contexts to explore potential applications.

2. **Training and Exploration:** Security personnel should thoroughly explore the system to gain a comprehensive understanding of its features and practical utility.
3. **System Updates and Upgrades:** Organizations implementing the system should ensure regular updates and consider upgrades to maintain its effectiveness and adaptability to emerging security challenges.

References

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2001). **Network Centric Warfare: Developing and Leveraging Information Superiority**. CCRP Publication Series.

Anderson, R. (2003). **Security Engineering: A Guide to Building Dependable Distributed Systems**. Wiley.

Anderson, C., & Agarwal, R. (2010). "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions." *MIS Quarterly*, 34(3), 613–643.

Barry, B. (1991). **People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era**. Harvester Wheatsheaf.

Bozeman, D. P., & Kacmar, K. M. (1997). "A Cybernetic Model of Impression Management Processes in Organizations." *Organizational Behavior and Human Decision Processes*, 69(1), 9-30.

Buzan, B. (2000). "The People, States, and Fear Paradigm Revisited." *Security Dialogue*, 31(3), 365–370.

Hadnagy, C., et al. (2011). **Social Engineering: The Art of Human Hacking**. Wiley.

Hubert, D. (1999). "The Links Between Human and Global Security." *Peace Review*, 11(1), 13–18.

Imobighe, T. A. (2003). **Civil Society and Ethnic Conflict Management in Nigeria**. Spectrum Books.

Kurose, J. F., & Ross, K. W. (2010). **Computer Networking: A Top-Down Approach**. Addison-Wesley.

Leary, M. R., & Kowalski, R. M. (1990). "Impression Management: A Literature Review and Two-Component Model." *Psychological Bulletin*, 107(1), 34–47.

Lippmann, W. (1944). **U.S. Foreign Policy: Shield of the Republic**. Little, Brown, and Company.

McNamara, R. S. (1968). "The Essence of Security: Reflections in Office." *Harper & Row*.

Posthumus, S., Von Solms, R., & King, M. (2007). "The Framework for the Governance of Information Security." *Computers & Security*, 26(3), 209–216.

Rogers, R. W. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change." *Journal of Psychology*, 91(1), 93–114.

Tikk, E. (2008). "The Impact of Cyber Attacks on National Security." *Cyber War, Estonia 2007*. Cooperative Cyber Defence Centre of Excellence.

Tikk, E., et al. (2008). "Cyber Attacks Against Georgia: Legal Lessons Identified." *NATO CCD COE Report*.

UNDP. (1994). **Human Development Report: New Dimensions of Human Security**. United Nations Development Programme.

Walt, S. M. (1991). "The Renaissance of Security Studies." *International Studies Quarterly*, 35(2), 211–239.

Zhuang, J. (2014). "Cyber Attack Theory and the Role of Moving Target Defense." *Proceedings of the 2014 ACM Workshop on Moving Target Defense*.

窗体顶端

窗体底端