ISSN: 2182-2069 / E-ISSN: 2182-2077

Blockchain-based Security Model to Mitigate the Risks of a Database for a Public Organization

T. Segundo M. Toapanta[1*], D. Rodrigo Del Pozo[2], Richard Romero Izurieta[3], Joseph A. Guamán[4], José A. Orizaga[5], Rocío M. Arellano[6], and María Mercedes Baño Hifóng[7]

[1*]Postgraduate Subsystems, Universidad Católica De Santiago De Guayaquil (UCSG), Guayaquil, Ecuador. segundo.toapanta@cu.ucsg.edu.ec, https://orcid.org/0000-0002-9041-0518

[2]Postgraduate Director, Universidad Estatal De Bolívar (UEB), Guaranda, Ecuador. rdelpozo@ueb.edu.ec, https://orcid.org/0000-0003-0418-2537

[3]Faculty of Education Sciences, Universidad Estatal De Milagro (UNEMI), Milagro, Ecuador. rromeroi@unemi.edu.ec, https://orcid.org/0000-0002-3387-6661

[4]Information Systems Department of the CUCEA, University of Guadalajara (UDG), Guadalajara, México. jguaman@armada.mil.ec, https://orcid.org/0000-0001-5791-2295

[5]Information Systems Department of the CUCEA, University of Guadalajara (UDG), Guadalajara, México. jose.orizaga@academicos.udg.mx, https://orcid.org/0000-0001-5649-5514

[6]Information Systems Department of the CUCEA, University of Guadalajara (UDG), Guadalajara, México. ma.maciel@academicos.udg.mx, https://orcid.org/0000-0002-5548-2073

[7]Postgraduate Subsystems, Universidad Católica De Santiago De Guayaquil (UCSG), Guayaquil, Ecuador. maria.bano@cu.ucsg.edu.ec, https://orcid.org/0000-0003-2904-3090

Received: February 27, 2024; Revised: April 24, 2024; Accepted: June 03, 2024; Published: August 30, 2024

Abstract

Effective information management is pivotal for public organizations, particularly in developing regions like Latin America, where cybersecurity capabilities are limited, leaving them vulnerable to increasingly sophisticated cyber threats, resulting in economic losses and reputational damage. This paper aims to design a security model leveraging Blockchain and Machine Learning technologies to mitigate the risks associated with information systems and databases in public organizations. Employing the deductive method and exploratory research, we analyzed scientific articles pertaining to security models and methodologies incorporating Blockchain and Machine Learning, culminating in the proposal of a novel security model tailored to public organizations. Additionally, we introduced a transaction management procedure for evaluating security models for public organization databases. The adoption of a layered model integrating Blockchain and Machine Learning significantly enhances security in public organizations, achieving effectiveness levels ranging from 80% to 98%. Furthermore, the amalgamation of Blockchain, Machine Learning, and artificial intelligence facilitates risk reduction and threat mitigation, thereby bolstering global security.

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 78-98.
DOI: *10.58346/JISIS.2024.I3.005*

*Corresponding author: Postgraduate Subsystems, Universidad Católica de Santiago de Guayaquil (UCSG), Guayaquil, Ecuador.

Keywords: Blockchain, Machine Learning, Database, Public Organization, Security of the Information.

1 Introduction

Effective information management is crucial for organizations, particularly those operating in the public sphere where citizen data is stored. To manage this information efficiently, organizations deploy database management systems (DBMS), which are pivotal for information security, aimed at mitigating risks and vulnerabilities associated with DBMS. Cyber incidents are on the rise, varying widely in nature. Consequently, organizations must implement technological and managerial controls to ensure asset protection (ESET, 2022). Particularly in developing countries, organizations face challenges due to their low level of cybersecurity capacity, leaving them vulnerable to increasingly sophisticated attacks and threats, resulting in substantial economic losses (Romero Izurieta et al., 2023).

Notable cyberattacks on public organizations in 2022 include a sensitive information leak from a Shanghai National Police database affecting over 1 billion citizens in China, a cyberattack targeting the Municipal Water and Sewerage Company of São Leopoldo, impacting over 230,000 citizens in Brazil, and a cyber-attack on the National Renewable Energy Center of Navarra de Sarriguren in Spain (Telefónica Cybersecurity & Cloud Tech, 2022). In Latin America and the Caribbean, 91% of organizations have reported at least one security incident, with organizations exhibiting low maturity experiencing more significant cybersecurity events (Deloitte, 2023).

o safeguard organizations from potential cyber threats and vulnerabilities, it is imperative to understand the threats and risks they face, enabling proactive prevention and response through organizational and technological solutions (Tagarev & Sharkov, 2019).

The architectures and security models of information systems and databases in public organizations are particularly vulnerable to cyber-attacks, which can have severe economic and reputational repercussions.

Why is a new security model necessary for the Database in a Public Organization?

Only a new security model can effectively mitigate the risks associated with information systems and databases, thereby enhancing trust, security, transparency, and traceability of shared data across networks (Javaid et al., 2022). To address the security and privacy requirements in data exchange scenarios within public organizations, we propose a security model that integrates blockchain and machine learning technologies.

This paper's main contributions are as follows:

1. Exploration of blockchain and artificial intelligence applications in public organizations.
2. Proposal of a modular security model integrating blockchain and artificial intelligence, comprising seven layers to ensure secure data exchange within organizational databases and information systems.
3. Provision of a transaction management procedure incorporating functionalities of blockchain and artificial intelligence layers.
4. Analyse the proposed model's security efficiency versus traditional and blockchain-only method.

The work is organized as follows: Section II describes the theoretical foundation and methodology applied. Section III presents the research findings. Section IV offers an analysis and comparison of the findings to other similar research published in the literature. Finally, Section V summarizes the findings and offers future work to further this research.

2 Materials and Methods

2.1. Materials

2.1.1. Databases

Databases (DB) and database management systems (DBMS) are two critical components for managing data storage, processing, and recovery in an organization, derived from transactional applications and other sources of information (Wannalai & Mekruksavanich, 2019). Figure 1 depicts the DBMS's interactions with the database, as well as the user, application, and service layers. The physical layer includes the files that govern the server database, which can be centralized or distributed (Narayanan et al., 2022). An organization's database management system (DBMS) is a complicated system composed of processes and memory that manage the tasks required by the user via applications and the service layer's business rules. To examine the number of layers in the architectural design of a system, an analysis of application and security requirements and demands is required.

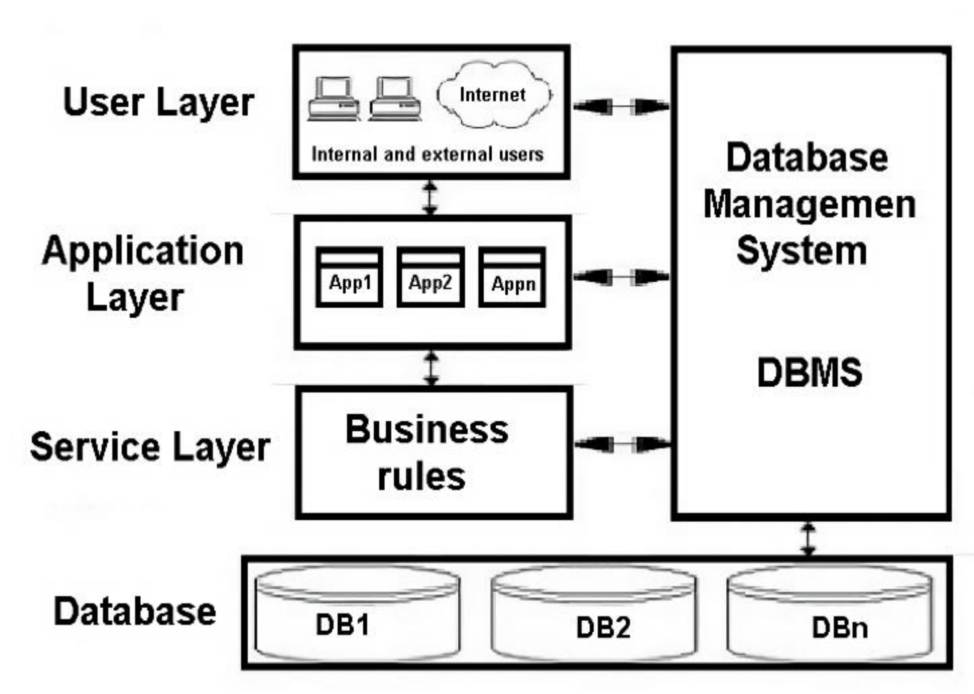

Figure 1: Database Architecture

Table 1: Attacks and Vulnerabilities to the Database

Reference	Attack or vulnerabilities	Solution with blockchain and AI
(Gamundani & Nekare, 2018; Gu et al., 2020; Toapanta et al., 2020)	SQL injection	The AI layer employs machine learning to determine abnormal patterns to prevent the execution of malicious SQL code and the blockchain authenticates and validates secure transactions.
(Castro & Pushpa Lakshmi, 2023; Gamundani & Nekare, 2018; Gharpure & Rai, 2022; Toapanta et al., 2020)	Denial of Services Distribution (DDoS)	The artificial intelligence layer can monitor traffic patterns and employ machine learning algorithms to identify and mitigate DDoS attacks in real-time.
(George et al., 2021)	Buffer overflow exploits	The AI layer has anomaly detection techniques to determine potential buffer overflows, and the blockchain imposes limits on transaction sizes.
(Anandhi et al., 2023; Pichikala et al., 2021)	Malware	The blockchain layer can ensure the integrity of transactions, while the artificial intelligence layer can analyze behavioral patterns to detect and prevent malware execution.
(Al-Barazanchi et al., 2020; Roja & Jayanthi, 2019; Toapanta et al., 2020)	Internal threats	The artificial intelligence layer can monitor internal user behavior and detect unusual activities, such as unauthorized access or suspicious configuration changes.
(Sánchez et al., 2020)	Exploitation of database software vulnerabilities	The blockchain layer can ensure secure updates, and the artificial intelligence layer can continuously assess potential vulnerabilities through code analysis and behavioral patterns.
(Castro & Pushpa Lakshmi, 2023)	Backup attacks	The blockchain layer can encrypt and authenticate backup data, and the artificial intelligence layer can monitor activities related to backups to detect suspicious behavior.
(Ahmad et al., 2022; Gharpure & Rai, 2022)	Weak audits	In the AI layer, audit logs can be analyzed to determine patterns in implementation failures, which are stored securely on the blockchain.

2.1.2. Database Attacks and Vulnerabilities

Integrating blockchain and artificial intelligence into a security model creates a robust environment that not only addresses specific vulnerabilities but also enhances the system's ability to adapt and defend against emerging threats. Table 1 outlines the most relevant attacks and vulnerabilities in databases.

2.1.3. Blockchain

Blockchain technology is gaining prominence, particularly for enhancing information security across various domains. Its key characteristics include decentralization, immutability, transparency, and peer-to-peer communication (Belotti et al., 2019; Rajasekaran et al., 2022).

Blockchain serves as an incorruptible digital ledger of transactions. Its advantages include transparency, trust, multiple copies of transactions, and a decentralized digital ledger. However, drawbacks such as high-power consumption, signature verification for every transaction, forks and outdated software, a trade-off between the number of nodes and user-friendly costs, and high transaction costs exist (Golosova & Romanovs, 2018). In Table 2, we highlight some reviewed studies on blockchain technology.

Table 2: Blockchain Literature Review

Reference	Category	Description
(Gangwani et al., 2023; Kumar et al., 2023; Suliyanti & Sari, 2023)	Blockchain applications	Models and mechanisms designed to enhance data security across various domains, including the Internet of Things (IoT).
(Belotti et al., 2019; Rajasekaran et al., 2022; Roussille et al., 2022; Toapanta et al., 2020; Zhang et al., 2021; Zhao, 2022)	Blockchain platform and architecture	Includes platforms such as Ethereum, Hyperledger Fabric, Corda, Eris, Ripple, ScalableBFT, Stellar, Dfinity, Tezos, and Sawtooth Lake. Blockchain architectures can be public, private, or federated.
(Aviv et al., 2023; Chenthara et al., 2020; Elisa et al., 2023; Lo et al., 2022; Maw et al., 2019)	Blockchain frameworks	Work environments that standardize concepts, platforms, practices, and criteria to address specific problems, serving as reference points.
(Pedrosa et al., 2021; Roussille et al., 2022)	Distributed computing with Blockchain	Utilizes blockchain technology in conjunction with distributed computing paradigms like cloud computing and grid computing.
(Belotti et al., 2019; Pachhaiammal Alias Priya et al., 2023; Rajasekaran et al., 2022; Suliyanti & Sari, 2023; Zhang et al., 2021)	Consensus protocols	Protocols governing how nodes in a blockchain network agree on the validity of transactions. Examples include Proof of Work, Proof of Stake, Delegated Proof of Stake, Byzantine Fault Tolerance (BFT), and Proof of Weight.
(Gupta et al., 2022; Muneeb et al., 2022)	Smart contracts	Programs stored on a blockchain that automatically execute predefined actions when specific conditions are met.

Figure 2 illustrates the operation of blockchain technology, starting from the initiation of a request from one of the involved parties until the completion of the transaction. Implementing blockchain technology necessitates consideration of the appropriate platform, architecture, and consensus protocol, tailored to the specific project requirements. Ethereum and Hyperledger Fabric are among the most widely utilized platforms, catering respectively to projects with publicly shared data and those with private or federated architectures (Zhao, 2022).

Smart contracts without human intervention are a fundamental component of blockchain (Gupta et al., 2022).

2.1.4. Blockchain and Artificial Intelligence (AI)

Blockchain and AI are two technologies that are present in multiple disciplines. Below is a description of several studies on their integration:

Chen et al., (2023), create a system that uses machine learning and blockchain for supply chain security. Peter et al., (2023), combine machine learning and blockchain to mitigate credit card fraud. Tsuruta et al., (2023), they use blockchain and machine learning algorithms in the systems to protect through automatic surveillance.

Other studies addressing new applications of blockchain, and AI are also examined, such as detecting malicious nodes in wireless sensor networks, predicting trends in the stock market, and protecting privacy in Internet-based systems of things. things. These studies describe the versatility and potential of combining blockchain with artificial intelligence technologies to address multiple challenges in a variety of fields. Below we detail the studies:

Puri et al., (2023), proposed an intelligent information system was proposed to support tourism, using blockchain, text mining, and machine learning models. Stodt et al., (2023), proposed a framework for data security and transparency in blockchain-secured dynamic machine learning channels is proposed. Witt et al., (2023), analyzed the advantages and limitations of decentralized and incentivized federated learning frameworks using blockchain are analyzed. Shah et al., (2023), used Blockchain and Machine Learning were used to ensure the security of the drug supply chain. Hu et al., (2023), presented an intelligent system for vaccine supply management was presented, through Blockchain, IoT and machine learning.

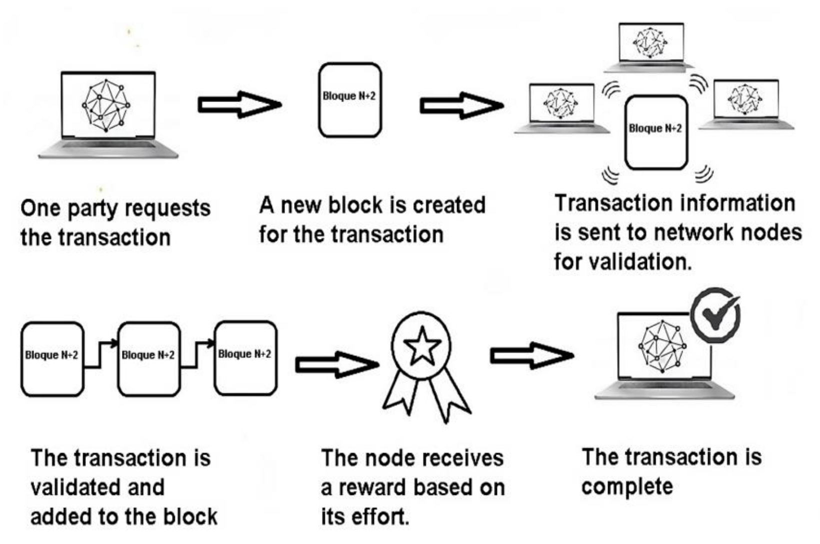

Figure 2: Blockchain Operation

2.2. Methods

2.2.1. First Phase

The initial phase involved an extensive search on official websites and scientific databases to understand the foundational aspects of database architecture. This included identifying the general structure of databases and compiling information on prevalent attacks and vulnerabilities affecting database security. Concurrently, we delved into literature on blockchain technology, exploring its features, benefits, drawbacks, platforms, architectures, and its integration with Artificial Intelligence (AI). Notably, we scrutinized studies focusing on the amalgamation of blockchain with AI to glean insights into mitigating security risks in public organization databases.

Utilizing the findings from this comprehensive literature review, we constructed Table 3, documenting the primary works referenced in our investigation. Modular Security Model shown in figure 3.

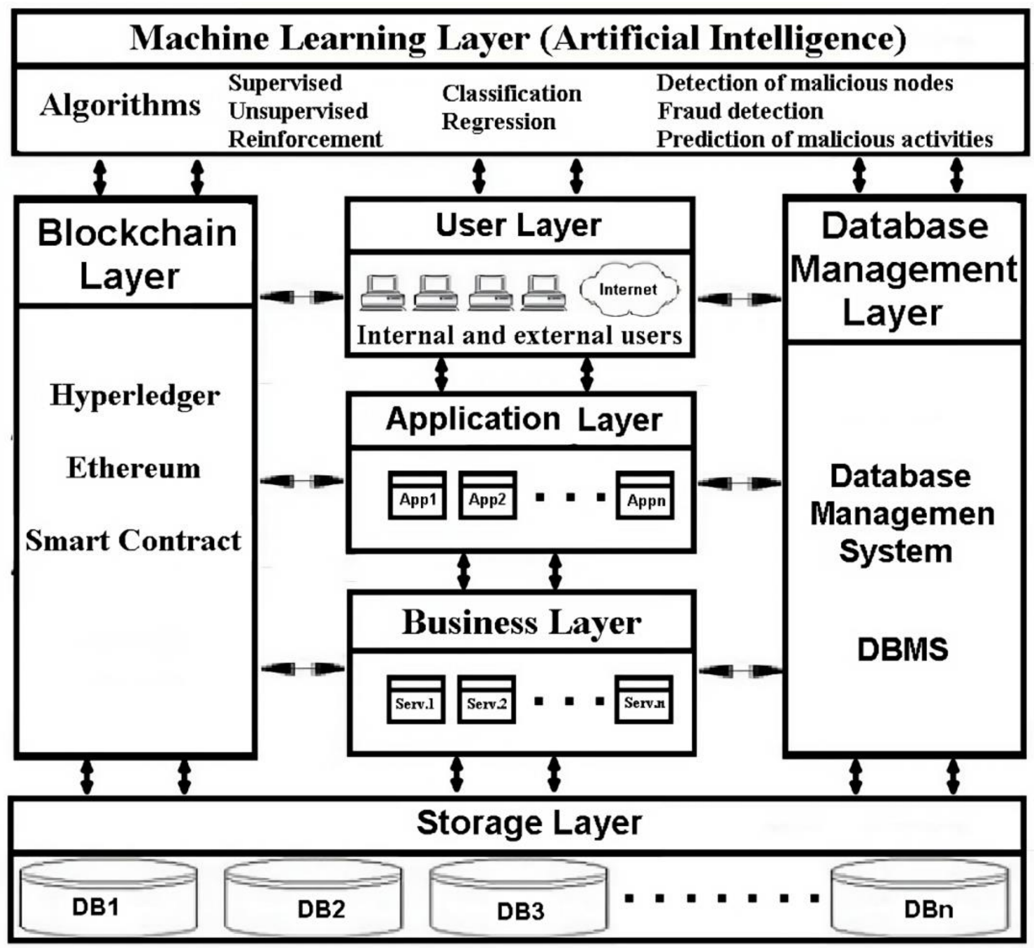

Figure 3: Modular Security Model

2.2.2. Second Phase

Building upon the insights garnered from the initial literature review, we employed the inductive-deductive method and logical reasoning in the second phase to devise a conceptual model ensuring the security of public organization databases. This model integrates advancements in Blockchain and AI Machine Learning (ML) technologies to foster transparency and secure communication among the organization and its internal and external stakeholders. Leveraging ML, we aim to anticipate suspicious and malicious activities by analyzing data collected from the blockchain and other layers.

During this phase, we formulated the architecture of the model, delineating its layered structure and elucidating the functionality of the security model from the perspective of mitigating database risks.

Table 3: Main Investigations Considered for the Proposed Model

Reference	Characteristics	Importance for our work
(Chenthara et al., 2020; Maw et al., 2019; Toapanta et al., 2020)	Proposes a security model for organization databases using hybrid blockchain.	We examined the advantages of employing a hybrid blockchain model specifically tailored for public organizations.
(Kumar et al., 2023)	Presents a scalable Blockchain architecture incorporating deep learning for network intrusion detection.	We recognize the significance of integrating blockchain and machine learning techniques to fortify security measures. The proposed architecture's scalability and integrity preservation align with our objectives.
(Elisa et al., 2023)	Introduces a decentralized e-government framework using consortium blockchain and artificial immune systems.	We acknowledge the potential of blockchain and machine learning integration to enhance security and privacy. The framework's focus on threat detection aligns with our proactive security approach.
(Achary & Shelke, 2023; Anandhi et al., 2023)	Proposes dynamic threat detection using machine learning.	We incorporate machine learning to bolster our model's ability to proactively identify and address security threats.
(Zhang et al., 2021)	Introduces a 3-tier architecture with hybrid blockchain for Central Bank digital currency (CBDC).	We adopt a similar approach, integrating a hybrid blockchain model by layers. Additionally, we reviewed the applied consensus mechanism for further insights.
(Peter et al., 2023)	Presents a method to detect fraudulent accounts on the Ethereum blockchain using machine learning.	We analyze the integration of blockchain with machine learning algorithms for fraud detection, considering potential applications in our security model.

2.2.3. Third Phase: Validation Through Simulation

Due to the sensitive nature of security incidents involving public organizations and the limited availability of statistics, validating the proposed security model required conducting several simulations using randomly generated data. These simulations were designed based on the criteria identified during the literature review phase.

To compare the effectiveness of our proposed Blockchain with AI security model against a model solely based on Blockchain and a traditional model lacking both Blockchain and AI, we utilized data from the OAS report on cybersecurity within the banking sector of Latin America and the Caribbean (refer to Table 4).

In our simulation:

- An organization employing a traditional security model is assumed to have a digital security detection and analysis capability ranging from 0 to 60%.
- An organization implementing a Blockchain security model is estimated to provide protection against digital security events within the range of 61 to 80%.
- Finally, an organization utilizing a Blockchain security model integrated with Artificial Intelligence is anticipated to offer protection against digital security events ranging from 81 to 100%.

These assumptions enable us to gauge the comparative effectiveness of our proposed security model against traditional and Blockchain-only approaches, providing insights into the potential benefits of integrating AI with Blockchain technology in safeguarding public organizations' digital assets.

We also perform another simulation of the effectiveness of the proposed model with a Python program considering the attacks and vulnerabilities in Table I, considering an arbitrary number of attacks.

Table 4: Digital Security Detection and Analysis

Percentage of Banks	Starting rank	Final rank
26%	0%	20%
7%	21%	40%
14%	41%	60%
26%	61%	80%
26%	81%	100%

3 Results

The following results were obtained:

3.1. Database Security Conceptual Model

A comprehensive conceptual security model for the database of a public organization has been developed. This model adopts a modular design with seven layers to ensure effective mitigation of the risks outlined in Table 1. Below are the details of each layer:

3.1.1. User Layer

This layer facilitates interactions between the public organization and both internal and external users, ensuring secure communication and transactions.

3.1.2. Application Layer

Providing network services to the organization's computer applications, this layer collaborates closely with the blockchain layer for key management and digital signature functionalities.

3.1.3. Business Layer

Housing the logic of the organization's applications and services, this layer interfaces with both the application and database layers. It also connects with the blockchain layer for secure smart contract management.

3.1.4. Storage Layer

This layer maintains a crucial connection with both the database and the blockchain layer because it is responsible for storing the data recorded by the organization's systems and databases.

3.1.5. Database Management Layer

This layer oversees the management of the organization's database management systems (DBMS), facilitating data management, transactions, and user permissions.

3.1.6. Blockchain Layer

This layer provides a decentralized, immutable, and transparent structure for secure data management. It uses a hybrid model with Hyperledger for internal authentication and Ethereum for external users. Implement smart contracts and use the DPoS algorithm for consensus. It interacts with all layers to ensure the security and traceability of transactions.

As a consensus mechanism, we use Delegated Proof-of-Stake (DPoS), where network users can choose delegates to validate blocks (Pachhaiammal Alias Priya et al., 2023). The operation of the DPoS algorithm depends on the voting of delegates, publication of blocks, and behavior of delegates. In voting, each user who has coins can vote for delegates in real time, and the reputation and the number of tokens that the delegates have are considered, the more tokens, the more votes they can receive. Once the delegates are elected, each can generate a new block according to a turn, for the new block they receive the economic incentive and distribute it with their voters. The performance of delegates is always evaluated by those who vote, and delegates can be expelled if they do something wrong and lose their prestige, good functioning is achieved, and abuses are avoided.

3.1.7. Machine Learning Layer

This layer implements machine learning algorithms for proactive detection of threats and malicious activities. It analyzes data from all layers, especially the blockchain layer, to predict and detect suspicious activities. It uses SVM, KNN, Naïve-Bayes, among others, for classification and prediction. This machine learning layer was created to manage the limitations of blockchain-based systems, thereby increasing the level of security and trust. The integration of these two technologies can guarantee the sustainability of the terms and conditions agreed upon in transactions. The fundamental basis is to update the machine learning models to be updated according to the blockchain network environment, extracting useful data from any part of the network, to be constantly processed. Cybersecurity problems are concerns that every organization has, which with the integration of blockchain and machine learning can be improved, with surveillance activities, through data that are analyzed in real time.

To classify users of public organization transactions that may be malicious, supervised learning is used. Online machine learning and deep learning are combined for anomaly detection. To preserve privacy, we also combine supervised learning, federated learning, and deep learning. Among the supervised learning algorithms, the Support vector machine (SVM) classifier can be used, K nearest neighbors (KNN), Naïve-Bayes, logistic regression, gradient boosting DT, random forests, additional trees, adaptive boosting (AdaBoost), Gradient Boosting, Random Forest, and Multi-Layer Perceptron (MLP), among others (Bin Sulaiman et al., 2022; Fadi et al., 2022). In the experimental part and applying the most used performance metrics to compare machine learning algorithms such as Accuracy, Precision and Recall we can choose the best algorithms (Sanni & Guruprasad, 2021).

3.2. Security Model from a Database Risk Perspective

A baseline security model has been devised to address database risks effectively:

3.2.1. Risk Identification

Thorough assessment of potential risks, including internal threats, software vulnerabilities, and various attack vectors.

3.2.2. Data Integrity

Utilization of the blockchain layer to ensure data integrity through immutable transaction recording. Security Model Baseline Risk Perspective shown in figure 4.

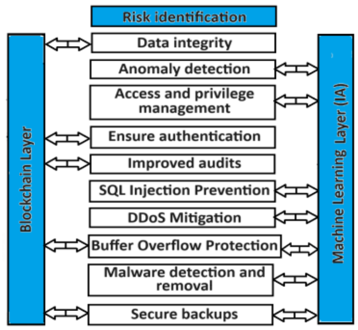

Figure 4: Security Model Baseline Risk Perspective

3.2.3. Anomaly Detection

Implementation of machine learning algorithms to detect anomalous activities, safeguarding against unauthorized access and unusual queries.

3.2.4. Access and Privileges Management

Establishment of strict access policies, with AI monitoring access patterns to enforce authorization controls.

3.2.5. Authentication Assurance

Blockchain technology is employed to authenticate users and transactions securely, preventing identity theft.

3.2.6. Improved Audits

Blockchain-based audit logging ensures secure and immutable records, aiding in identifying security weaknesses and suggesting enhancements.

3.2.7. SQL Injection Prevention

Filters and validations implemented in the AI layer mitigate the risk of SQL injection attacks.

3.2.8. DDoS Mitigation

Real-time traffic monitoring and AI algorithms identify and mitigate DDoS attack patterns.

3.2.9. Protection against Buffer Overflow

Strict limits on transaction sizes in the blockchain layer prevent buffer overflow attempts.

3.2.10. Malware Detection and Removal

Behavioral analysis by the AI layer enables early detection and removal of malware.

3.2.11. Secure Backups

Blockchain encryption and authentication ensure the security of backup data, with AI monitoring backup-related activities for threats.

3.3. Transaction Management Procedure

The transaction management procedure orchestrates the handling of services and transactions within public organizations. Controlled by the blockchain layer and monitored by the machine learning layer, this procedure ensures the integrity and security of transactions. Figure 5 shows the process described below:

1. **User Transaction Request:** The procedure initiates with a user's transaction request, for which the private key undergoes validation.
2. **Access Validation:** Upon successful validation, the user interacts with the system and database of the public organization.
3. **Transaction Creation:** If access is authenticated, a new transaction is created. The blockchain validates the terms and conditions while the user provides the required data.
4. **Blockchain Validation:** After validating the data, terms and conditions, the blockchain receives the transaction data and validates the public key.
5. **Transaction Record:** The transaction is recorded in both the blockchain and the public organization database if all validations are successful.

Throughout this process, the machine learning layer remains active and works with other layers to detect fraud, suspicious activities, and potential malicious behavior, thereby improving security measures at all stages of the transaction lifecycle.

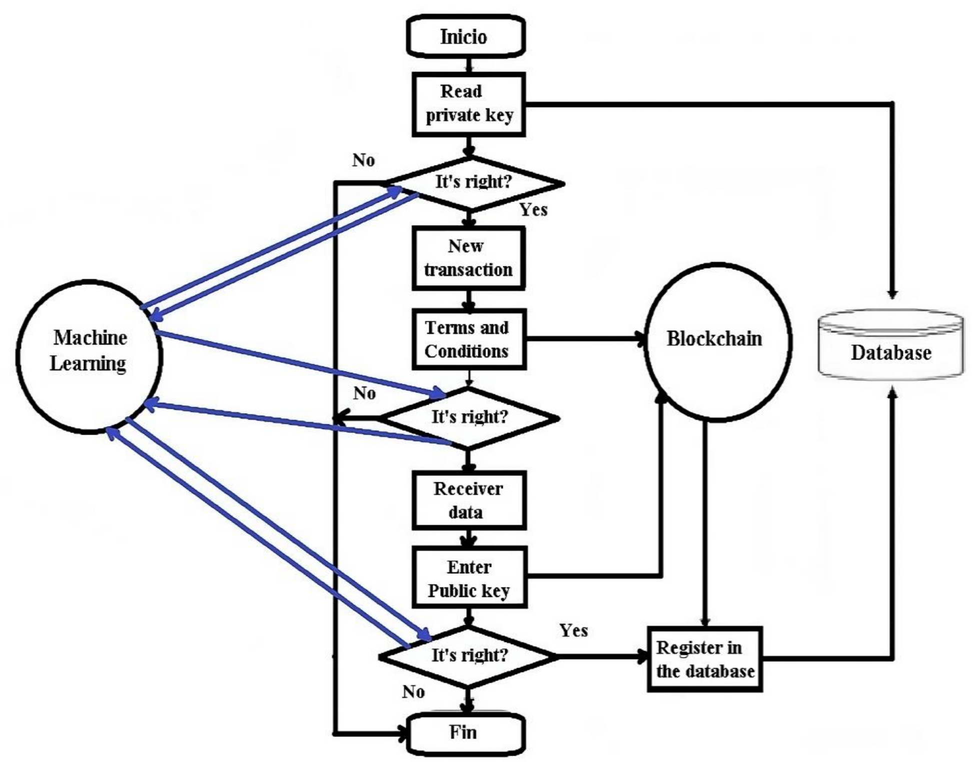

Figure 5: Procedure for Managing Transactions.

3.4. Model Evaluation

The model evaluation includes the simulation of twenty random scenarios based on empirical data. This evaluation analyzes the security effectiveness of three different models: a traditional model, a blockchain model, and a model that integrates blockchain and machine learning. The following is a summary of the results in Figure 6:

- The suggested model is effective: the proposed model, which uses blockchain and machine learning, reaches values of 80% to 98%. This demonstrates its ability to reduce security risks and increase overall protection.
- Efficiency of the blockchain-only model: The model based solely on blockchain technology demonstrated moderate efficiency, with values from 60% to 88%. Although it significantly improves security compared to conventional methods, it does not provide the complete protection that the integrated model offers.
- Efficiency of the traditional model: The traditional model without blockchain has the lowest efficiency, with values from 32 to 73%. This shows that conventional security methods are fragile when it comes to adequately protecting against today's cyber threats.

Furthermore, a detailed comparison of the security models created using a Python program is shown in Figure 7. This comparison demonstrates the superiority of the proposed model in detecting and addressing a variety of attacks and vulnerabilities. Furthermore, it confirms its effectiveness in improving organizational security measures. Simulations of Random Situations shown in table 5.

Table 5: Simulations of Random Situations

Scenarios	**Traditional model**	**Blockchain model**	**Blockchain and AI model**
1	46	78	86
1	46	78	86
2	49	66	88
3	41	70	90
4	43	65	86
5	44	80	91
6	59	73	94
7	52	73	91
8	44	74	90
9	45	79	87
10	58	61	87
11	49	67	84
12	58	68	81
13	46	74	90
14	42	69	91
15	49	63	86
16	44	79	93
17	44	67	95
18	60	66	95
19	59	62	87
20	59	67	84

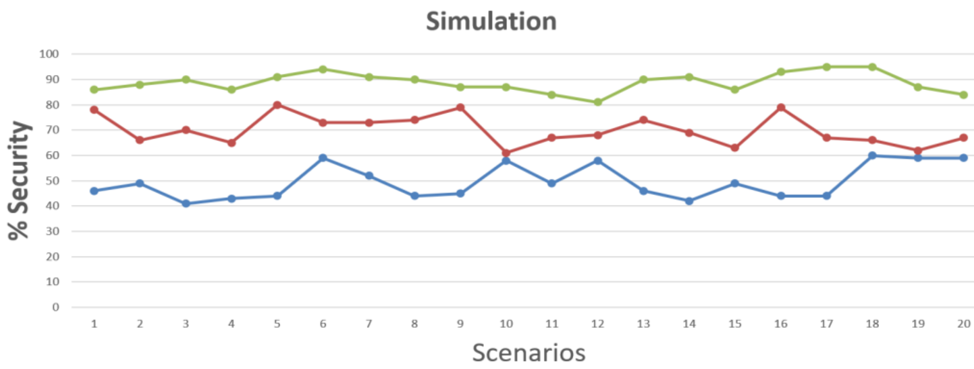

Figure 6: Model Comparison

4 Discussion

The suggested model represents a breakthrough in protecting digital transactions and data storage within a public organization's system. Trust, security, transparency and traceability of transactions carried out within the organization's network have improved significantly. The proactive threat detection capabilities of the machine learning layer and the comprehensive security measures provided by blockchain technology are the main contributors to this improvement.

The model effectively mitigates attacks and vulnerabilities of traditional systems by using Blockchain smart contract functions to ensure information traceability and security. Machine learning and blockchain layer integration create a secure environment for the organization's information system and database, offering robust protection against cyber threats.

The model prioritizes the application of blockchain and machine learning technologies to protect the privacy of sensitive data. The model protects sensitive transactions and data by incorporating neural networks and federated learning, as found in the literature (Bin Sulaiman et al., 2022).

The literature review found several scientific articles showing similar models that focus on creating secure architectures and models using blockchain and machine learning technologies (see Table 6). This demonstrates a growing trend towards incorporating these sophisticated technologies to improve cybersecurity measures in a variety of industries, including public organizations.

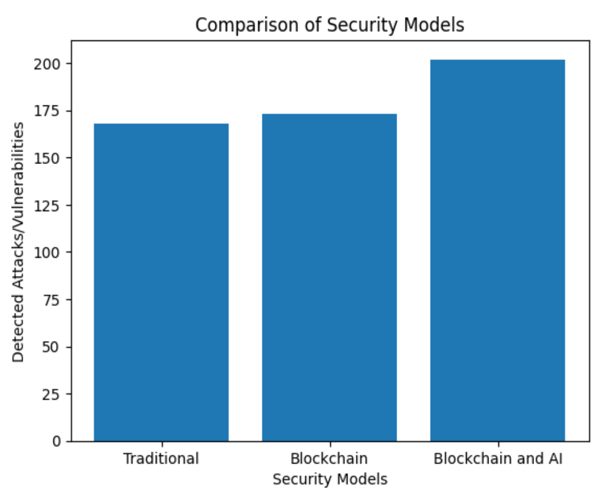

Figure 7: Comparison of Security Models

Table 6: Comparison with other Investigations

Reference	Research proposal	Our research
(Toapanta et al., 2020)	They improved database security using a hybrid blockchain with 99.5% efficiency based on simulations.	Our model also considers a hybrid blockchain approach, but additionally addresses security risks using machine learning techniques.
(Kumar et al., 2023)	They integrated blockchain and deep learning to design an intrusion detection system with a test accuracy close to 99%.	We integrate blockchain with machine learning techniques into our model, extending it to a series of algorithms to prevent and detect malicious activities at a variety of layers and operations.
(Elisa et al., 2023)	They integrated a consortium blockchain with artificial immune systems, with threat detection rates of 92.72 to 97.65%.	In our research we also incorporate blockchain with machine learning techniques, expanding its application to a variety of algorithms for the prevention and detection of malicious activities at different layers and operations.
(Anandhi et al., 2023)	They used machine learning to automate the detection and classification of new malware, with an average accuracy of 98.4%.	Our model considers the automation of threat detection and prevention in one layer, but also integrates blockchain security in information management.
(Peter et al., 2023)	The detection method gave accuracy results with different classifiers between 90.8 and 99.2%.	This model only includes credit card fraud detection; Our focus encompasses global security.
(Achary & Shelke, 2023)	The model achieved a performance of 97.74% in detecting fraud in banking transactions using machine learning.	Our model considers global threat detection at the machine learning layer, integrated with blockchain security.

Its comprehensive security approach combines blockchain with machine learning techniques to address a wide range of threats across multiple layers and system operations, which highlights our research. Our proposed model achieves impressive efficiency results of 80% to 98% by covering all aspects of security, including authentication, data integrity, anomaly detection, and prevention of specific attacks such as SQL injection and DDoS.

Compared to the models indicated in Table 6, our research shows that it provides significant security coverage. While other models can solve specific security issues, they sometimes lack the holistic approach that our model offers, which includes numerous layers and approaches for complete protection supported by blockchain technology and artificial intelligence.

The model we propose employs a seven-layer approach. This framework allows for comprehensive security control at all stages of data processing. The models in Table 6 have fewer layers, implying less rigorous security management. It is essential It should be noted that multi-layered models, such as ours, may be more difficult to create and manage. But we must point out that complex security architectures allow for greater protection of information in public organizations.

The proposed approach is based on the constant innovation of cybersecurity, we provide a consistent solution as an alternative to mitigate risks, vulnerabilities and threats. The integration of blockchain and machine learning enables public organizations to have a reliable security architecture for digital transactions.

5 Future Works and Conclusion

In the short term, we will continue with the research, applying the proposed security model to perform experiments with real data from a determined number of public organizations according to the population and sample that is decided to be carried out in a timely manner.

It was concluded that the proposed security model is an alternative to guarantee the privacy, traceability, transparency and integrity of data. The integration of blockchain and artificial intelligence allows mitigating information risks, to improve the capabilities of organizations in their management.

The results obtained in this research provide a comprehensive response to information security problems in public organizations, with an innovative and adaptable approach to combat cyber threats.

One of the key features of the suggested security model is the use of a hybrid blockchain that combines Hyperledger and Ethereum to implement smart contracts and automate transaction traceability. Machine learning helps prevent security issues by recognizing suspicious and malicious activities at various levels of the system network. The excellent results (80% to 98%) indicate the safety efficiency of the model.

In summary, the suggested security model provides a solid framework for improving information protection in public organizations. The model fosters transparency and trust among users by integrating blockchain and artificial intelligence technologies to provide sophisticated defense against cyber threats. Further research and experimentation will undoubtedly refine and validate the effectiveness of this model in real-world environments.

References

[1] Achary, R., & Shelke, C. J. (2023). Fraud Detection in Banking Transactions Using Machine Learning. *International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, 221–226. https://doi.org/10.1109/IITCEE57236.2023.10091067

[2] Ahmad, A., Saad, M., Al Ghamdi, M., Nyang, D., & Mohaisen, D. (2022). BlockTrail: A Service for Secure and Transparent Blockchain-Driven Audit Trails. *IEEE Systems Journal, 16*(1), 1367–1378. https://doi.org/10.1109/JSYST.2021.3097744

[3] Al-Barazanchi, I., Jaaz, Z. A., Abbas, H. H., & Abdulshaheed, H. R. (2020). Practical application of IOT and its implications on the existing software. *7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI)*, 10–14. https://doi.org/10.23919/EECSI50503.2020.9251302

[4] Anandhi, V., Vinod, P., Menon, V. G., ER, A. K., Shilesh, A., Viswam, A., & Shafiq, A. (2023). Malware Detection using Dynamic Analysis. *International Conference on Advances in Intelligent Computing and Applications (AICAPS)*, 1–6. https://doi.org/10.1109/AICAPS57044.2023.10074588

[5] Aviv, I., Barger, A., Kofman, A., & Weisfeld, R. (2023). Reference Architecture for Blockchain-Native Distributed Information System. *IEEE Access*, *11*, 4838-4851.

[6] Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials, 21*(4), 3796–3838. https://doi.org/10.1109/COMST.2019.2928178

[7] Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of Machine Learning Approach on Credit Card Fraud Detection. *Human-Centric Intelligent Systems, 2*(1), 55–68. https://doi.org/10.1007/s44230-022-00004-0

[8] Castro, S., & Pushpa Lakshmi, R. (2023). Enhanced Rsa (Ersa): An Advanced Mechanism for Improving the Security. *Intelligent Automation & Soft Computing*, *36*(2), 2267- 2279.

[9] Chen, Y.M., Chen, T.Y., & Li, J.S. (2023). A Machine Learning-Based Anomaly Detection Method and Blockchain-Based Secure Protection Technology in Collaborative Food Supply Chain. *International Journal of E-Collaboration (IJeC)*, *19*(1), 1–24.

[10] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *Plos One, 15*(12), e0243043.

[11] Deloitte. (2023). Global Future of Cyber Survey. https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html

[12] Elisa, N., Yang, L., Chao, F., Naik, N., & Boongoen, T. (2023). A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity. *IEEE Access, 11*, 8773–8789.

[13] ESET. (2022). Security Report Latinoamérica 2022. https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf

[14] Fadi, O., Karim, Z., Abdellatif, E. G., & Mohammed, B. (2022). A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments. *IEEE Access, 10*, 93168–93186. https://doi.org/10.1109/ACCESS.2022.3203568

[15] Gamundani, A. M., & Nekare, L. M. (2018). A review of new trends in cyber attacks: A zoom into distributed database systems. *In IEEE IST-Africa Week Conference (IST-Africa)*.

[16] Gangwani, P., Bhardwaj, T., Perez-Pons, A., Upadhyay, H., & Lagos, L. (2023). On the Convergence of Blockchain and IoT for Enhanced Security. *In Artificial Intelligence in Cyber-Physical Systems*, 25–49.

[17] George, G., Kotey, J., Ripley, M., Sultana, K. Z., & Codabux, Z. (2021). A Preliminary Study on Common Programming Mistakes that Lead to Buffer Overflow Vulnerability. *IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1375–1380. https://doi.org/10.1109/COMPSAC51774.2021.00194

[18] Gharpure, N., & Rai, A. (2022). Vulnerabilities and Threat Management in Relational Database Management Systems. *5th International Conference on Advances in Science and Technology (ICAST)*, 369–374. https://doi.org/10.1109/ICAST55766.2022.10039599

[19] Golosova, J., & Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. *IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, 1–6. https://doi.org/10.1109/AIEEE.2018.8592253

[20] Gu, H., Zhang, J., Liu, T., Hu, M., Zhou, J., Wei, T., & Chen, M. (2020). DIAVA: A Traffic-Based Framework for Detection of SQL Injection Attacks and Vulnerability Analysis of Leaked Data. *IEEE Transactions on Reliability*, *69*(1), 188–202. https://doi.org/10.1109/TR.2019.2925415

[21] Gupta, D., Kumar, B., Sharma, A., & Kumar Mishra, D. (2022). Smart Contracts: Violations, Applications and Comparisons. *Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, 964–971. https://doi.org/10.1109/ICICICT54557.2022.9917893

[22] Hu, H., Xu, J., Liu, M., & Lim, M. K. (2023). Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning. *Journal of Business Research, 156*, 113480. https://doi.org/10.1016/j.jbusres.2022.113480

[23] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *Bench Council Transactions on Benchmarks, Standards and Evaluations, 2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

[24] Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., & Islam, A. K. M. N. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *Journal of Parallel and Distributed Computing, 172*, 69–83.

[25] Lo, S. K., Liu, Y., Lu, Q., Wang, C., Xu, X., Paik, H. Y., & Zhu, L. (2022). Toward trustworthy ai: Blockchain-based architecture design for accountability and fairness of federated learning systems. *IEEE Internet of Things Journal*, *10*(4), 3276-3284.

[26] Maw, A., Adepu, S., & Mathur, A. (2019). ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive and Mobile Computing*, *59*, 101048. https://doi.org/10.1016/j.pmcj.2019.101048

[27] Muneeb, M., Raza, Z., Haq, I. U., & Shafiq, O. (2022). SmartCon: A Blockchain-Based Framework for Smart Contracts and Transaction Management. *IEEE Access, 10,* 23687–23699. https://doi.org/10.1109/ACCESS.2021.3135562

[28] Narayanan, U., Paul, V., & Joseph, S. (2022). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. *Journal of King Saud University-Computer and Information Sciences*, *34*(6), 3121–3135.

[29] Pachhaiammal Alias Priya, M., Rajulu, N. S., Jayanthi, S., & Kavitha, G. (2023). Blockchain Oriented Hybrid Architecture for Crowdsource Model. *International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, 1454–1459. https://doi.org/10.1109/ICSCSS57650.2023.10169151

[30] Pedrosa, M., Lebre, R., & Costa, C. (2021). A performant protocol for distributed health records databases. *IEEE Access, 9,* 125930–125940.

[31] Peter, A., Manoj, K., & Kumar, P. (2023). Blockchain and Machine Learning Approaches for Credit Card Fraud Detection. *5th International Conference on Smart Systems and Inventive Technology (ICSSIT),* 1034–1041. https://doi.org/10.1109/ICSSIT55814.2023.10060999

[32] Pichikala, S. M., Rachana, G., Sanjanapatel, H., Shanu, S., & Vineeth, N. (2021). Malware Detection using Blockchain Technology. *2nd International Conference for Emerging Technology (INCET),* 1–4. https://doi.org/10.1109/INCET51464.2021.9456161

[33] Puri, V., Mondal, S., Das, S., & Vrana, V. G. (2023). Blockchain Propels Tourism Industry—An Attempt to Explore Topics and Information in Smart Tourism Management through Text Mining and Machine Learning. *Informatics, 10*(1), 9. https://doi.org/10.3390/informatics10010009

[34] Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments, 52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

[35] Roja, C., & Jayanthi, P. N. (2019). Syslog Daemon for Security Event Monitoring using UDP Protocol. *3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA),* 1349–1354. https://doi.org/10.1109/ICECA.2019.8821956

[36] Romero Izurieta, R., Toapanta Toapanta, S. M., Caucha Morales, L. J., Baño Hifóng, M. M., Gómez Díaz, E. Z., Zambrano Vizuete, O. M., Mafla Gallegos, L. E., & Orizaga Trejo, J. A. (2023). Prototype to Identify the Capacity in Cybersecurity Management for a Public Organization. *Advances in Science, Technology and Engineering Systems Journal*, *8*(1), 108–115. https://doi.org/10.25046/aj080113

[37] Roussille, H., Gürcan, Ö., & Michel, F. (2022). AGR4BS: A Generic Multi-Agent Organizational Model for Blockchain Systems. *Big Data and Cognitive Computing*, *6*(1). https://doi.org/10.3390/bdcc6010001

[38] Sánchez, M. C., De Gea, J. M. C., Fernández-Alemán, J. L., Garceran, J., & Toval, A. (2020). Software vulnerabilities overview: A descriptive study. *Tsinghua Science and Technology*, *25*(2), 270–280. https://doi.org/10.26599/TST.2019.9010003

[39] Sanni, R. R., & Guruprasad, H. S. (2021). Analysis of performance metrics of heart failured patients using Python and machine learning algorithms. *Global Transitions Proceedings*, *2*(2), 233–237. https://doi.org/10.1016/j.gltp.2021.08.028

[40] Shah, Y., Verma, Y., Sharma, U., Sampat, A., & Kulkarni, V. (2023). Supply Chain for Safe & Timely Distribution of Medicines using Blockchain & Machine Learning. *5th International*

Conference on Smart Systems and Inventive Technology (ICSSIT), 1123–1129. https://doi.org/10.1109/ICSSIT55814.2023.10061049

[41] Stodt, F., Stodt, J., & Reich, C. (2023). Blockchain Secured Dynamic Machine Learning Pipeline for Manufacturing. *Applied Sciences, 13*(2), 782. https://doi.org/10.3390/app13020782

[42] Suliyanti, W. N., & Sari, R. F. (2023). Blockchain-Based Double-Layer Byzantine Fault Tolerance for Scalability Enhancement for Building Information Modeling Information Exchange. *Big Data and Cognitive Computing, 7*(2), 90. https://doi.org/10.3390/bdcc7020090

[43] Tagarev, T., & Sharkov, G. (2019). Computationally intensive functions in designing and operating distributed cyber secure and resilient systems. *In Proceedings of the 20th International Conference on Computer Systems and Technologies*, 8-18.

[44] Telefónica Cybersecurity & Cloud Tech. (2022). State of Security Report 2022 H2.

[45] Toapanta, S. M., Quimis, O. A. E., Gallegos, L. E. M., & Arellano, M. R. M. (2020). Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks. *IEEE Access*, *8*, 169367-169384.

[46] Tsuruta, Y., Akiyama, K., Shinkuma, R., & Mine, A. (2023). Blockchain framework for managing machine-learning models for 3D object detection. *In IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 704-705. https://doi.org/10.1109/CCNC51644.2023.10060161

[47] Wannalai, N., & Mekruksavanich, S. (2019). The application of intelligent database for modern information management. *In Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON)*, 105-108.

[48] Witt, L., Heyer, M., Toyoda, K., Samek, W., & Li, D. (2023). Decentral and Incentivized Federated Learning Frameworks: A Systematic Literature Review. *IEEE Internet of Things Journal, 10*(4), 3642–3663. https://doi.org/10.1109/JIOT.2022.3231363

[49] Zhang, J., Tian, R., Cao, Y., Yuan, X., Yu, Z., Yan, X., & Zhang, X. (2021). A Hybrid Model for Central Bank Digital Currency Based on Blockchain. *IEEE Access, 9*, 53589–53601. https://doi.org/10.1109/ACCESS.2021.3071033

[50] Zhao, Z. (2022). Comparison of hyperledger fabric and ethereum blockchain. *In IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, 584-587. https://doi.org/10.1109/IPEC54454.2022.9777292

Authors Biography

Prof. Segundo Moisés Toapanta Toapanta, has a Doctor in Information Technology (PhD) from the University of Guadalajara-Mexico, Master in Communications Management and Information Technology from the National Polytechnic School (EPN), Computer and Information Technology Engineer. He carried out his doctoral research stays at the Polytechnic University of Cartagena (UPCT) Spain and at the Faculty of Systems Engineering of the National Polytechnic School. Research Professor in the Postgraduate Subsystem of the Catholic University of Santiago de Guayaquil (UCSG), Guest Professor in postgraduate studies at the University of Guadalajara in Mexico, Guest Professor in Graduate Studies at several Universities in Ecuador, Peru, Mexico and Spain, Director and Co-director of Master's and Doctoral thesis. He is an accredited evaluator and researcher, categorized Principal 1 in the RNI-Senescyt. Research lines: Strategic Alignment of ICT, Distributed Systems, Networks, High Performance Computing, Information Security, Cryptography, Cybersecurity, Cyberbullying, Cybercrime, Blockchain Technologies and Applications.

Prof. Rodrigo Humberto Del Pozo Durango, is an Engineer in Computer Science and Computer Science, has a Master's degree in Computer Science and Electronic Commerce, is a Local Main Contact (LMC) Cisco UEB Academy and a Cisco UEB Instructor in CCNA, CCNA Security and Cyber Operations. I was Vice Dean of the Faculty of Administrative Sciences, Business Management and Information Technology, I was a Member of the Board of Directors of the Faculty of Administrative Sciences, Business Management and Information Technology, I was a Member of the Academic Commission of the Faculty of Administrative Sciences, Business Management and Information Technology, I was Director of the School of Systems Engineering, I was Director of the Institute of Information and Communication Technologies, He is a Member of the Academic Commission of the University, He is a Member of the Research and Linkage Commission of the University, I was Administrative Director of the Driving School of the State University of Bolívar, I was Director of the National Transit Agency ANT, Professor at the State University of Bolívar from 1999 to the present in the Faculties of Administrative Sciences, Business Management and Information Technology and Educational Sciences. Participation in various local, national and international training events.

Prof. Richard Romero Izurieta, is a Professor at the Milagro UNEMI State University. He has a Doctor in Applied Mathematical Statistics from the National University of Tumbes, a Master in Information Systems with a mention in Data Science from Hemisferios University, a Computer Engineer from the Escuela Superior Politécnica del Litoral, a Master in Business Administration with a mention in International Business. from the University of Guayaquil. He has 20 years of professional experience in the IT area, carrying out technological projects for different public and private companies. He has 10 years of experience in different universities in Ecuador, where he has directed undergraduate and graduate theses. He has participated in some national and international conferences and conferences, he has published scientific articles in high-impact journals, his lines of research focus on three large areas: Administration, Statistics and Computing.

Prof. Joseph Alexander Guaman Seis, is a PhD student in Information Technology at the University of Guadalajara in Mexico, Master in Information Technology at the National Polytechnic School (EPN), Master in Computer Security at the Litoral Polytechnic School (ESPOL), Computer Science and Computer Science Engineer. He is currently Director of Information Technologies at the University of the Armed Forces of Ecuador. He has held several positions at an operational, tactical and strategic level in different divisions of the Ecuadorian Navy. He has the military rank (Naval) of Specialist Frigate Captain. in Computer Science in the Ecuadorian Navy. His research lines are: Computer Security, Cyberterrorism, Cybercrime, IT Infrastructures, New Blockchain Technologies.

Prof. José Antonio Orizaga Trejo, obtained his master's degree in Information Systems, Networks and Telecommunications at the University of Guadalajara De México, stay of Doctoral Research in Telecommunications Engineering at the University of Vigo, he obtained the degree of Doctor in Information Technologies at the University of Guadalajara of México. He is a professor of Distributed Systems at the University of Guadalajara, Coordinator of the Master in Information Technologies at the University of Guadalajara, CUCEA. He researcher and Professional in next-generation Convergent Technologies, fields of specialization in Cloud Computing, IoT over Smart Cities, Networking and Telecommunications, Security Systems in HPC and Financial Services. Research Areas: Cloud Computing, IoT over Smart Cities, Networking and Telecommunications, Security Systems in HPC and Financial Services.

Prof. Rocio Maciel Arellano, is a Research Professor in the Information Systems Department of the CUCEA University of Guadalajara (UDG) and is currently Coordinator of Linking and Talent at the Center for Innovation in Smart Cities of the UDG. She is a member of the academic nucleus of the Doctorate in Information Technology, of which she was coordinator from 2013 to 2016, obtaining her accreditation in the National Quality Standard (PNPC) by the National Council of Science and Technology (CONACYT). He has extensive experience in the field of virtual education through online platforms and has directed several research and postgraduate thesis, in addition to supporting projects in Information Technology. Additionally, it has scientific publications and has participated in international conferences and panels. Manage national and international projects. Research Areas: Smart Cities, Education and innovation, Virtual environments, Information Security, Information Technologies.

Prof. María Mercedes Baño Hifóng, is Doctor in Strategic Business Administration from the Pontifical Catholic University of Peru, Master in education and educational innovation. She also has a master's degree in international public accounting and a diploma in the same specialty from the University of Guadalajara (Mexico), a degree in economics with a mention in business management. She has extensive experience as a financial consultant for national and international companies. She has participated in presentations, publication of scientific articles, book chapters and books contributing from the financial and accounting perspective to the sustainable development of the business environment. She is the functional coordinator of the Vice President for Research and Postgraduate Studies at the Catholic University of Santiago de Guayaquil, where she participates in inter-institutional research projects at the local and regional levels. She is the leader of the research table at the Finance and Accounting Observatory of the Accreditation Council for Business Schools and Programs (ACBSP). Research Areas: Strategic Alignment, International Business, Information Security, Business Administration and Information Technology.