IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Analysis for the Evaluation and Security Management of a Database in a Public Organization to Mitigate Cyber Attacks

Segundo M. Toapanta [1], **Omar A. Escalante** [1], **Luis E. Mafla** [2] **and Rocío M. Arellano** [3]

[1]Department of Computer Science, Salesian Polytechnic University (UPS), Guayaquil, Ecuador
[2]Faculty of System Engineering, National polytechnic school (EPN), Quito, Ecuador
[3]Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, Mexico

Corresponding author: Segundo M. Toapanta (stoapanta@ups.edu.ec).

Funding

ABSTRACT In data handling, security and privacy are essential for database administrators and users that own their information. Information about security models or architectures was analyzed for databases that minimize Cyber Attacks. The problem is that security models deployed in databases in public organizations suffer from computer attacks due to vulnerabilities in their security management systems. Data providers often publish the information for research purposes, publishing compromises on the privacy of the data of users registered in the entities. There are many security techniques for databases based on data encryption processes in transactions, however, the techniques found compromise information. The development of the document used the deductive method and exploratory research technique that allows us to study the information in the articles presented. In this document we have proposed a Security Model Assessment Prototype for Databases, a Prototype of Security Management Architecture in Blockchain for a Database, a Database Security Algorithm, a Logical Structure of the Management System in Blockchain, and a Prototype to mitigate cyberattacks. The use of a hybrid blockchain model provides the system with the optimal security that public organizations in relation to test results performed with a 99.50% security effectiveness. The simulations presented in this document were conducted based on in-depth studies and the data were randomly placed with a range according to the study results based on real-world situations.

INDEX TERMS Blockchain, cyber attacks, cyber security, data base, public organization.

I. INTRODUCTION

Database is important for the management of an organization, the availability of this data serves to have an agile response to people looking for a better service; the correct implementation of a database in public organizations help to achieve the objective, so public organizations need to implement security measures; public entities have the problem of information theft, duplication of information, denial of service, without obtaining information in a timely manner; cyber attackers are looking for a breach in the system to enter and have several tools for accessing the systems or databases of organization [1]. Some of Latin American countries adopt laws that guarantee data protection guidelines that are stored in each of the public organizations; and sometimes, such as in electoral processes, the cyber attacker enters these processes in such a way that attackers make changes to the number of votes of one or more candidates; these changes hurt a nation, as in the United States that blames Russia for hacking the emails of Democratic party and also the presidential candidate; in Latin America there is most possible manipulation in the results of the electoral process due to the electoral system implemented in the Government [2]. In Ecuador, block network models are established that allow confidentiality and scalability to ensure information security [3], government of China implements security measures on blockchain models, to assist in the contribution of each organization in China and generate changes in the different services of country [4]. Database is a collection of data that become of different types; this data is structured in such a way that it makes it easy to use in the different systems that are implemented in companies or organizations [5].

The problem is that security models deployed in databases in public organizations suffer from computer attacks due to vulnerabilities in their security management systems.

Why is necessary an Analysis for the Security Assessment and Management of a Database in a Public Organization to Mitigate Cyber Attacks?

To mitigate vulnerabilities and threats in the databases of the various Public Organizations, in the event of a possible attempt to infiltrate the attacker into the system; for the most vulnerable departments to counter the attack in a timely manner, with the instructions of the security prototype in the face of a cyberattack.

Related and reviewed articles regarding database evaluation, management and cyberattacks are as follows:

DBSAFE—An Anomaly Detection System to Protect Databases From Exfiltration Attempts [1], Analysis of Cyberattacks in Public Organizations in Latin America [2], Proposal of a Model to Apply Hyperledger in Digital Identity Solutions in a Public Organization of Ecuador [3], The Application of Blockchain Technology in E-government in China [4], Design and Implementation of a New Database Security Model Based on Hopping Mechanism [5], Defeating the Database Adversary Using Deception - A MySQL Database Honeypot [6], Impact on Administrative Processes by Cyberattacks in a Public Organization of Ecuador [7], Prototype to Mitigate the Risks of the Integrity of Cyberattack Information in Electoral Processes in Latin America [8], Anomaly detection of access patterns in database [9], Efficient and Effective Security Model for Database Specially Designed to Avoid Internal Threats [10], Blockchain-Based Safety Management System for the Grain Supply Chain [11], NutBaaS : A Blockchain-as-a-Service Platform [12], Integration of Blockchains with Management Information Systems [13], IoT Data Management and Lineage Traceability A Blockchain-based Solution [14], A Lightweight Vulnerability Scanning and Security Enhanced System For Oracle Database [15], Anomaly Detection in Large Databases Using Behavioral Patterning [16], Countermeasure of Statistical Inference in Database Security [17], Data Masking System Based on Ink Technology [18], Database Security with AES Encryption, Elliptic Curve Encryption and Signature [19], Hybrid Database Design Combination of Blockchain And Central Database [20], Security Concept in Web Database Development and Administration [21], Securing Big Data in the Age of AI [22], The Implementation of Negative Database as a Security Technique on a Generic Database System [23], Protection of Database Security via Collaborative Inference Detection [24], Identity Management for e-Government [25], A Security Evaluation and Certification Management Database Based on ISO/IEC Standards [26], Database Security in Private Database Clouds [27], Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing [28], Workload Management in Database Management Systems: A Taxonomy [29], Analysis of Identity Management Systems Using Blockchain Technology [30], A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations [31], PassBio : Privacy-Preserving User-Centric Biometric Authentication [32], Exploiting Information-Centric Networking to Federate Spatial Databases [33], Fingerprint Biometrics From Newborn to Adult: A Study From a National Identity Database System [34], Medical Image Infosecurity Using Hash Transformation and Optimization-Based Controller in a Health Information System: Case Study in Breast Elastography and X-Ray Image [35], A Secure and Efficient Distributed Storage Scheme SAONT-RS Based on an Improved AONT and Erasure Coding [36], A Secure Cloud Storage Framework With Access Control Based on Blockchain [37], Blockchain-Based Outsourced Storage Schema in Untrusted Environment [38], Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance [39], GDPR-Compliant Personal Data Management: A Blockchain-Based Solution [40], Search Condition-Hiding Query Evaluation on Encrypted Databases [41], Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain [42], SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN [43], Storage Mechanism Optimization in Blockchain System Based on Residual Number System [44], Performance of OnPrem Versus Azure SQL Server: A Case Study [45], Fair Data Transactions Across Private Databases [46], A Blockchain Privacy Protection Scheme Based on Ring Signature [47], Comprehensive Survey on Big Data Privacy Protection [48], A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure [49], A Visual Analysis of Research on Information Security Risk by Using CiteSpace [50], Improved Generalization for Secure Data Publishing [51], Performance Evaluation of a Combined Anomaly Detection Platform [52], CryptSQLite: SQLite With High Data Security [53], An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study [54].

The objective is to provide an analysis to evaluate and manage the security of a database in Public Organizations to mitigate the Cyber Attack.

It is used the deductive method and the exploratory research technique that allow us to perform the work and study the information in the articles presented.

The results are an Evaluation prototype of a databases security model, an Architecture prototype of security management on Blockchain for a database, an Algorithm prototype of security for databases, a Logical structure of the management system on Blockchain and a prototype to mitigate Cyber Attacks.

It is concluded that the prototype of the proposed architecture on a hybrid blockchain model provides an optimal security system for public organizations; according to the architecture simulation, the database has greater effectiveness up to 99.50% in security, this simulation was performed by means of random data based on real situations.

II. MATERIALS Y METHODS

A. MATERIALS

The authors designed the detection of anomalies and attack response that are presented in the company; this system created database profiles that recorded normal user behavior with the Database and a log of possible malicious behaviors that did not match user data; the model was responsible for monitoring data traffic and used the security techniques implemented; thanks to this system, they were detected in advance by a comparison of unusual behavior [1].

The authors proposed a model for countering denial-of-service cyberattacks on public organizations; they implemented a network prototype that controlled the arrival traffic of requests that intended to reach the servers; a system of security layers that controlled access to the network to prevent denial of service was implemented; an unusual traffic analysis algorithm was generated to identify malicious and legitimate packets; as a result, data needed to establish security platforms were obtained in the face of potential attacks [2].

The authors designed a blockchain model to ensure information from a public organization; they implemented a prototype model that helped with identity certification and had a network administrator; diagrams were made identifying user movements and interaction between them, and a logical representation of the detailed data was made; as a result they had a reliable and scalable system, here private storage is allowed in a decentralized way [3].

The author analyzed adaptation for a blockchain-based system in current e-government; they determined that by implementing a blockchain system on government platforms, different sectors could have reliable management of records; they established physical security measures as better risk management, this helped maximize security levels; as the result of the analysis was determined that implementing blockchain could have reliable information [4].

The authors designed a jump mechanism model for the security of a database; they implemented security methods for authentication data and were contained in a hop node; these hops were performed at certain times and randomly through the ports; here the client and server were synchronized with the help of an algorithm; with this implementation they got greater connection security between the client and the database server [5].

The authors implemented a trap system for the protection of an organization; they used a scheme of two organizations that had access between them; a cheating system was implemented in a table that was not used by the system and in an email containing sensitive information; the movements that emerged in these two systems were stored for prompt response to a possible attack; using this system they detected and collected information in order to take security measures [6].

This article discussed the impact of cyberattacks on the different processes of a public organization in Ecuador; the way the cyber attacker makes the entrance to an organization interface was analyzed; different contingency plans were explored, this helped the organization as data recovery plans, responses against cyberattack or disaster recovery; as a result of this analysis, control strategies were identified for possible attacks by public entities [7].

The authors proposed a prototype risk mitigation of a cyberattack on electoral processes; the patterns of attacker for committing the crime, such as data collection, searching for a vulnerability in the system, were analyzed, and an array was implemented for the assessment of different levels of risks; according to this calculation, security measures were put in place in the system and the implementation of the prototype; as a result, a better adaptation of the security model was achieved according to the levels to mitigate cyberattacks [8].

The authors implemented a system of intrusion detections in the database; they analyzed unusual patterns from the attacking user and analyzed the number of unusual queries with the number of queries that are normally made; as a result, historical data was visualized to determine whether traffic flow was unusual at a certain time; thanks to the implementation of the detection system, users will be monitored to visualize possible manipulations in the database [9].

The authors proposed a security model to mitigate high-performance internal threats; they implemented security rules describing policies for users, users interact directly with the database; Based on security model analyses, permissions are set for the user to access a certain part of the base; as a result of the deployment you will get a base and tables will not be accessed if you do not have the permissions by the database administrator [10].

The authors proposed a blockchain-based architecture for better information management; they conducted a study that helped them determine a unique coding system towards objects and placed identifiers; due to large amounts of logs, a multimode storage mechanism was implemented and data security was provided and could not be tampered with; as a result of the model reliable data was obtained with less log load in the database [11].

The authors developed a platform using a blockchain-as-a-service system through cloud computing; identified layers that provided services as databases to infrastructure, business solutions in an agile manner; hybrid cloud implementation provided security to hinder external attack; cloud computing service effectively improved the flaws of a block-as-a-service system, and improved data reliability and threat detection [12].

The authors analyzed a public, private and consortium blockchain system; they were identified that public blocks do not need authorization to interact with the system, and transparency in the data is allowed; private blocks are looking for ways to maintain confidentiality of their data and consortium blocks sought control organizationally; as a result of the analysis, better information management is sought from companies that applied a blockchain system [13].

The authors designed IoT device data management based on a blockchain system; using a code the identifiers were generated for each device, made possible a better record of the device data; this data will not be manipulated by external users; as a result, a storage system was effectively obtained with information and device management with the intruder defense feature is possible [14].

The authors proposed a database capacity and security improvement system for the detection of potential threats; vulnerability reports were analyzed, identified that users accessing the database acquired certain privileges; these users made changes to the base because of this vulnerability; repair methods were applied in the system, this generated a technical report; this mechanism resolved the processes of detecting vulnerabilities in the system [15].

The authors proposed a database anomaly detection model; by processing instructions that are set in events, here they helped detect anomaly, then viewed suspicious users, and sent a report of user activities; after analyzing the data the movements of the attackers were visualized, this model helps companies that aim to have a secure system of effective detection of database anomalies [16].

The author proposed a model of data concealment against internal threats; user-made queries were determined and made tables wanted to access, the model determined whether the user has authorized access to the table they want to access; on the other hand the administrator handles queries and determines the attributes of the database considered as sensitive data; as a result, an information management system was obtained that only privileged users have permission to access [17].

The authors proposed a data masking system, they implemented an algorithm that generated public and private keys and stored codes in a file containing all the generated codes; by using this process the attackers did not detect the users, this is because the information that is considered confidential is masked; this made changes to the original data with similar data as a result the system kept its original format and the information in the system is more efficient [18].

The authors proposed methods of storing and retrieving database information; the confidentiality method ensures that information is only accessed by authorized users, encryption determines the security of the data; encryption methods are applied to the elements, using a random key, the base will use a cryptographic security type; as a result of implementing this cryptography model for data storage in a secure way [19].

The authors proposed a hybrid model to improve database performance with the use of chain locks; This method implemented an interface that was used to manage networks, determining administrator roles and users; through the system, access could be given to manage blockchains and the list of users that exist in the database; as a result they determined that this model be implemented on any organization [20].

Different threats mitigated database security were analyzed; being a model that is in development, being a database over the network, data security is very susceptible to cyberattacks; different reliability, data integrity, availability issues were analyzed; this analysis helped establish the different control methods that the system was implemented in the web databases [21].

The authors proposed a model that allows organizations security management in the database; the intrusion detection model obtained information that served to protect data that is confidential and vulnerable; this helped to create data control policies, and unauthorized access detection was also performed on the system; with these results a broad view of how the method implemented towards security was worked on in the database [22].

This article proposed a generic database system for the growth of current databases with a security layer; implementing allowed the system to have control over user input data; this enabled a security model capable of providing ease of data management at the base; as a result of the implementation, a system capable of managing the database with sensitive data was obtained, impenetrable security measures are applied [23].

A module was proposed that draws understanding from data dependency, schemas, and environment knowledge; according to the structure of the database the data dependency is extracted; knowledge of the environment is drawn from semantic links; the model builds knowledge based on extracted information; this information serves for data inference and relationships between attributes [24].

The authors explored information for national identification management and online access for Libya; with this information they proposed and developed a model of issue of identification numbers; compared their model with other identification schemes; expose impersonation as a major vulnerability; this work is aimed at the national identity authority and governments [25].

The authors used ISO/IEC standards to evaluate system evidence, these are tangible, important and confidential documents; here the evaluators analyze the contents efficiently, this evidence can have losses, changes, different versions [26].

The authors proposed database security; even though audit logs are stored on different servers; the problem is that agents scan database logs and send them to different agents and servers; the proposal uses multiple databases and sends the logs to the central server and end users connect to this server [27].

The focus of this research is to detect in real time a malware and rookit attack through analysis of information from virtualized services; the approach analyzes the characteristics of big data; the system verifies the attack characteristics and determines the presence of the attack through logistic regression and belief transmission [28].

The authors provided an analysis of load management systems in the databases; they applied taxonomy to evaluate and classify the techniques of managers; between revised processes are schedules, accesses and controls; they also highlighted the strengths and weaknesses of the reviewed managers [29].

The authors reviewed three blockchain-based identity tools and presented digital identity concepts; the comparative features are user control, supervised use, identification, technology benefits, integration and user experiences; among the highlighted approaches are identity control, a non-centralized identity, simple verification; they affirmed the need for identity management systems on blockchain [30].

The authors reviewed the references about health systems on blockchain, they presented general architectures, described the Ethereum and Hyperledger platforms, authentication, data storage, information security and privacy [31].

This document proposed a biometric security scheme aimed at the user and allows them to encrypt their own data; the storage provider cannot decrypt the biometric data of user, this does not allow the attacker to see the data; uses distance in X and Y vectors for encryption; authors ensure security and privacy, and affirmed their efficiency in pcs and phones [32].

This document presented an architecture for federating spatial databases, such as the formation and grouping of common data; through a framework for a secure data center made up of layers [33].

The authors assessed fingerprints to identify people of any age, including minors; they tested two hundred thousand footprints belonging to 134 thousand people; for the purpose of being able to identify people in access from any age regardless of their age advance or change in muscle mass [34].

To protect patient confidentiality, data security, prevent unauthorized access, prevent theft or data manipulation; the authors applied multi-secret keys and a controller that helps encrypt or decrypt digital medical images in a health database; the architecture encrypts the images in the sender, it travels encrypted to the recipient, the receiver decrypts the image and saves it in the database [35].

The authors presented a distributed storage scheme with erased encoding; the information in this schema performed processes that encoded using algorithms, generated a key, and divided it into blocks; the shared blocks were rebuilt and with the generated key the packets were decoded; the implementation of this scheme provided security for storage, but with problems with denial-of-service detection, blocks affected by attackers cannot be recovered [36].

The authors proposed a cloud storage framework with access controls with the use of blockchain technology; the accounts that provided the blockchains are externally owned with private keys generated by administrators; Smart contracts provided storage security with algorithms according to the schemes posed by the authors; the algorithm posed by encryption attributes prevented attackers from having unauthorized access to storage [37].

TABLE II
EVALUATION MODELS

Model	Process	Efficiency %	Ref.
Model of inference	Extracting information from the database	Collaboration Level 98.9%	[24]
National identification	National identification number in Libya, vulnerability analysis.	Model only	[25]
Management assessment	Adoption of ISO/IEC standards for a database	Qualitative model	[26]
Security system	System uses two security agents, first agent is on central server, and second agent passes data.	Model only	[27]
Detect real-time attacks on the database	Analysis of possible route characteristics, determine attack presence	0.08ms to detect	[28]
Management systems review	Database workload	Qualitative analysis	[29]
Blockchain identity model	Analysis of 3 identity management models	Qualitative comparisons	[30]
Biometric access system	They use vectors n dimensions of real numbers to store biometric information; 2-phase process	Biometric register Vector n= 300 en 900ms	[32]
Federation of space databases	Data security across layers	Confidence tests at 95%	[33]
Fingerprint identification and comparison	Fingerprint usage from any age	Tests in children 92.64% confidence; tests in adults 98.39% confidence	[34]
Medical image security architecture	Image encryption for submission; decryption of images at the reception	Cryptography less than 4 seconds	[35]

Table II contains database security assessment models or architectures; the efficiency of models in times or percentages is highlighted; others there are only qualitative analyses.

The authors proposed reliably storing and verifying data by using blockchain in the system; the system implemented an algorithm that collects metadata for the creation of the blocks, the administrator performed a signature validation process with the data entered; the blocks were also modified according to the number of messages that were presented; as a result reliability was obtained in the storage of the data according to the verification throughout the process [38].

The authors performed a blockchain analysis with a focus on systems with large data storage; the use of blockchains provided reliability in the data that is stored in the system, the stored data was encoded; Smart contracts ensure the encapsulation of data and according to the permissions of the administrator, users participated in the blockchain network; as a result of the analysis, the use of blockchain ensured that the information was handled appropriately [39].

The authors proposed the implementation of a blockchain technology-based data management system in accordance with the general data protection regulation; users allowed the service provider to have their data collected, the provider managed the data that was used to transact; a third party providing the system services to users that interacted with the service provider; the design implemented resulted in a reliable and secure management of personal data [40].

The authors provided query protocols for private databases with a focus on the confidentiality of the data that the user queries; the customer requested a data query and the method provides security on the data using encryption; the random database is secured by end-to-end encryption keys; as a result of the implementation of the security protocol in queries, more reliable data and data hiding were obtained from potential threats [41].

The authors proposed blockchain segmentation for block storage with a single copy; the model allowed the blockchain blocks to be segmented according to the amount allowed by the model, the segments took the number of nodes in the system; the allocation of storage in the blocks was entered according to the links; as a result, storage requirements could be reduced according to the blockchain system, without compromising system security [42].

The authors proposed an attack detection method based on elastic grouping; implementing the method provided greater security according to the different detection methods; the method helped eliminate redundant information in the system, early detection of the attack provided an accuracy of the behavior of attackers; as a result, an automatic behavioral analysis was obtained, identifying the traffic of the attack [43].

The authors proposed a mechanism to optimize system-based storage for node volume reduction; the consensus algorithm ensured the distribution of data in a public blockchain system; the raft algorithm guaranteed the subdivision of the nodes according to the term of each node was chosen a leading node and response nodes; as a result the mechanism used ensured a reduction in the volume of data storage for the security of stored information [44].

The authors proposed an analysis on the use of an on-premises database against a cloud-hosted database and the management of both cases; a test base was implemented for each environment, they implemented modules to identify the number of user interacting with the data, developing an application for according to the on-premises or cloud model had a different structure; analysis of the comparison between the different bases was carried out under the supervision of the administrators visualizing the advantages of each database [45].

The author proposed a scheme for practical tasks in secure information transactions; two separate processes were implemented, the advance delivery of the data that allowed the data to be delivered in an encrypted form from one end to the other with an identifier in the desired data; the acquisition of tags that I identify to the data by means of a label for quick search of information; the implementation of the schema helped that the transaction of the data is carried out in a secure way from the user to the database [46].

The authors proposed an information protection scheme using a blockchain system; implemented a data storage protocol to ensure user privacy in the system; used smart contracts for network monitoring, with the implementation of smart contracts obtaining results from compliance with established policies; as a result of the implementation of the ring signing scheme they obtained a system with a high privacy rate in user data [47].

The authors proposed the use of data mining without affecting the information that is stored in the database; the data obtained privacy in the moment that transferred to other data mining servers, the user information was transmitted without affecting privacy; data detection and extraction processes were carried out using a system-supported format; as a result of the implementation, it was possible to have a degree of privacy in the data at the time of data manipulation [48].

The authors proposed an analysis of a technological computer security system for the identification of internal threats; they determined the behavior of anomalies found through a thorough study using the qualitative methodology; the study determined cases with the best data reliability and information quality; as a result of the study, the need to educate users that handle information and commit information to third parties was identified [49].

The authors proposed an analysis of the structure, development and study of information security risk; the number of countries that implemented information security was determined, in accordance with network and information technology; the effective way to improve a level of security to the database was analyzed; as a result of the analysis, useful ways were used in accordance with global statistics to effectively manage information security risks [50].

The authors in this article proposed the analysis of hierarchies to preserve the data and information of people; experiment with a set of published data for detailed review according to the methods employed by the authors; they created the intervals in the search results of the tables for group creation according to the method to anonymize the data; as a result, three hierarchical models were obtained according to the number of nodes found to overcome the limitations [51].

The authors proposed an evaluation of the different anomaly detection algorithms to mitigate risks in systems; information was obtained on how the implementation of algorithms helps filter that happens in communication channels; determined the use of few resources in the use the hybrid anomaly detection algorithm; we compare a model and the algorithm is used independently for attack detection; as a result of the analysis, it was determined that the hybrid algorithm is accepted according to the threat detection efficiency [52].

The authors proposed the implementation of reliable execution environment technology with an authentication system to improve security in the database manager; the security system was implemented independently, each database was stored separately for each application in the system; applications and the manager communicated through a secure channel, and was assured in the execution of the consultations; as a result, an authenticated encryption system was implemented to protect the confidentiality of data [53].

The authors proposed implementing an architecture using blockchain in a database for the availability of records; they used a mechanism for users to view stored logs and blocks were encrypted for the transfer of records to the database; an Ethereum blockchain system was also used for the transfer of information according to the identifiers of each block; as a result it was determined that records cannot be altered by any user when the data is viewed or transferred [54].

B. METHODS

To carry out the study, the different articles were analyzed to list the possible threats that a database may suffer, according to the results of the analysis it was possible to determine the following.

1) LIST OF ATTACKS

Computer attacks are established as malicious acts by a group of people seeking the vulnerability of the system to cause damage to an infrastructure.

TABLE III
CYBERSECURITY ATTACKS

Model	Process	Ref.
DoS	Denial of service prevents the user from accessing the database.	[2] [21]
Unauthorized access	The objective is to access the system that ignores user authentication measures.	[3] [14]
Cyber espionage	How the attacker obtains sensitive information from a user without permission.	[6]
Black hat	The objective is to obtain sensitive data from vulnerable users for malicious purposes.	[7]
Grey hat	The objective is to identify system vulnerabilities.	[7]
Social engineering	Attackers obtain sensitive information through users and have access to the database.	[8]
Information theft	It is the way the attacker gets information from a database.	[16] [17]
Internal threats	Users in a company have access to sensitive data for manipulation.	[18]
Malicious attacks	The data is intercepted by the attacker, altered, and then sent to the recipient.	[19]
SQL injection	The objective is to manipulate the database without the need for authorization	[21]
Abuse of Excessive Privilege	The user is granted permissions that do not agree with their policies.	[21]

Table II described the different attacks that affected the different database systems in the revised articles.

2) GLOBAL ATTACK REPORT

Data on total losses for the past 5 years were collected, the total loss was determined to be $10.2 billion; the formula determined that the average reported threats are 341,523.6 per year; the data collected is globally and dollar loss can be calculated based on threats found and reported.

Figure 1 has a study of the last 5 years in relation to money involvement, here in 2019 a loss of $3.5 trillion was reached with a rate of 467,361 complaints [55].

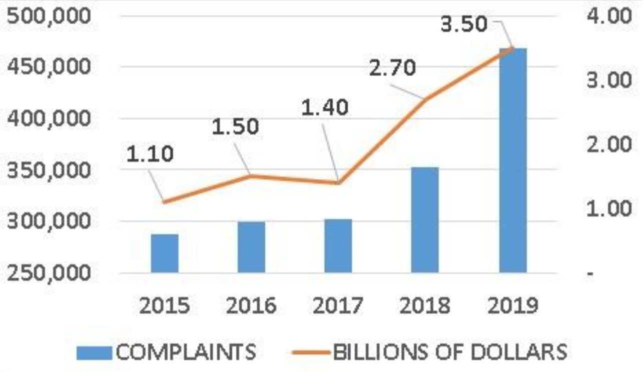

FIGURE 1. **Reports vs billions of dollars globally.**

The countries that are affected by cyberattacks are: first, this UK obtained the highest rate 93,796 victims; in tenth place is Argentina with an index of 578 victims; in 20th place is Russia with a rate of 349 victims.

The mathematical sustenment for measuring Reports vs Millions of Dollars globally is formula (1)

$$AT = \frac{\sum_{i=1}^{n} x_i}{n} \tag{1}$$

Here:
AT is the average billions of dollars lost over the years.
n is the number of years.
x is the function based on the number of years.

3) PROPOSAL

- Evaluate security models
- Targeted for a public organization
- Adopting Blockchain technology to manage security
- Define an architecture to manage the security of a database

- Define the steps to run security management

III. RESULTS

The results of this phase are:

- Evaluation prototype of a database security model
- Blockchain security management architecture prototype for a database
- Algorithm prototype of security for databases
- Logical structure of the management system on Blockchain
- Prototype to mitigate Cyber Attacks

A. EVALUATION PROTOTYPE OF A DATABASE SECURITY MODEL

From the references, we adopt some specific *functions* or *parameters* to form the evaluation prototype, below, we detail each parameter:

User definitions, roles, system parts, and system access were adopted from the functions to save and direct people or process entries to the system and database [25].

User activity log, the structures of activities and actions were adopted to save in a log the movements of people browsing between the application options or make requests to the database; it also proposes an alarm process to system administrators called *Alarms in bad user actions* [26].

Access reports and real-time monitoring a process was adopted to save the movements of users; this process must have as parameters the user, name of the process, date, time, action taken, identification of the computer or device [28].

Structured database or independent database was adopted the idea to know on the basis of the database, because the identification of users must be validated and certified in organized data: in addition from this reference the function is proposed to determine whether the security access is encrypted [30].

Encrypted or biometric security access was adopted the model to know if an encrypted security access exists, the identity credentials must be encrypted for better user security [35]; the study revised the model to see if there is a biometric access scheme for the evaluated system [32], [34].

Our structure is easy to evaluate to determine whether a platform, systems or application has the minimum-security functions to protect the database, this structure is auditable [27].

A list of 12 items was proposed to assess security in a database, the evaluator or auditor should measure each item with 0 or 1; 0 means that it does not have the function; 1 means that if you have the function; the list of functions is described in Table VI.

TABLE IV
EVALUATION PROTOTYPE

Function	Score
Definition of users	0 or 1
Role definition	0 or 1
Definition of systems	0 or 1
Defining access to the system	0 or 1
User activity log	0 or 1
Access reports	0 or 1
Structured database	0 or 1
Independent database	0 or 1
Alarms in user bad actions	0 or 1
Real-time monitoring	0 or 1
Adaptable to any data structure	0 or 1
Encrypted or biometric security access	0 or 1
Score	

Table VI described the different assessment points to the security model.

Three types of measure were established by ranks; all binary results of the elements are sued, and the score is given according to the following range:

Between 0 and 4 is low score

Between 5 and 8 is half score

Between 9 and 12 is high score

The score of the evaluation is expressed in formula (2)

$$P_m = \sum_{i=0}^{y} \frac{\sum_{f=1}^{n} f}{(1+s)^y} \tag{2}$$

$$Score = P_m * (md + mi + mp) \tag{3}$$

Here:

y are the years of the system.

n is the number of functions; k is every function.

s is the number of systems connected to the database.

md are the months of system design and database.

mi are the months of system and database implementation.

mp are the months of unit testing of the system and database.

In the example below is a simulation with random values 0 or 1; in the evaluation prototype, the result of this measure with the lowest score obtained, the evaluation of a security system in an organization was carried out; and thanks to the results, the scenarios were analyzed and the decision of administration is to improve security; system results were also analyzed while performing better with the highest score; with data collection is evaluated in the field of action and the prototype used to achieve an improvement in the system.

The application of the evaluation prototype is interpreted in functions that have zero value, must be attended, considered, and implemented; the score is to publicize how under the system in your database security.

Example:

TABLE V
EVALUATION PROTOTYPE

Funtion	Point
Definition of users	1
Role definition	1
Definition of systems	1
Defining access to the system	1
User activity log	0
Access reports	0

Structured database		1
Independent database		1
Alarms in user bad actions		0
Real-time monitoring		0
Adaptable to any data structure		0
Encrypted or biometric security access		
	Score	6

From the previous score the organization is during its security management; for this reason, you should review, improve, or propose a log structure, reports, alarms, and encrypted.

In the example below, the result of this measure was achieved an assessment of the security system and thanks to the results the scenarios could be analyzed and actions were taken to improve security; system results were also analyzed while performing better with the highest score; with the collection of data were evaluated in the field of action, the prototype used and we determined an improvement in the system.

B. ARCHITECTURE PROTOTYPE OF SECURITY MANAGEMENT ON BLOCKCHAIN FOR A DATABASE

A five-layer architecture prototype was proposed to secure public organization information and better manage sensitive data.

User layer: With this layer we identify how users in the organization or external users interact with the system and database; these media are mobile devices, desktop, laptops, tablets.

Application layer: All system applications in the public organization are stored in this layer; this app is based on a client-server model, here are web pages, desktop apps, mobile apps, remote access applications.

Service layer: Defines business rule and data manipulation language elements in the organization; provides the availability of the data, through SQL statements the data is stored, modified, or deleted.

Database layer: In this layer you will find the different servers of the organization, here are the data accessed by users and database administrators; different servers were determined according to the organization that needs to be deployed.

Blockchain layer: here is the system that will help manage database security through Blockchain platforms; the platform helps to manage users belonging to the organization users outside the organization.

In the prototype presented has a hybrid Blockchain network, formed by the Hyperledger and Ethereum platforms in the system applications that users use; for the private part the Hyperledger platform will be used for the management of users belonging to the public organization; through income credentials stored on nodes, private users access the information that only the Blockchain administrator allows; while Ethereum provides external users with access without the need for some kind of credential, through the intelligent contract provided by the platform; this contract will be an agreement between the organization and the user to access the information.

Figure 2 establishes the idea of management security on a hybrid architecture; is composed of Hyperledger for the accesses of the internal staff and Ethereum for external access.

Administrator roles: Takes care of system definitions and database servers in your organization in the face of potential threats; design, documentation, and compliance verification of security policies for the system and users; perform maintenance of the data of organization to ensure availability, integrity, and availability; constantly monitor security alert systems to gain control and counteract a possible unauthorized access attack; keep track of users, passwords, and access to apps in your organization; performs the execution of a backup schedule of data stored on the databases; through the audit of the information system, the administrator performs a system scan to identify potential system vulnerabilities; the study of this audit improves the system to achieve application and database efficiency; by retrieving data, the administrator plans to back up the data in the event of potential database corruption; this data can be restored to another alternate server; with data export and import, the administrator extracts or imports the data to the same server or to alternate servers; with data masking, data is encrypted, the blockchain manager identifies the data that this process should be performed; sensitive data is usually encrypted as login credentials.

Examples of architecture in public organizations:

Ministry of Education: here the managers of the institution through Hyperledger access with their credentials to the system; the Blockchain administrator provides privileges according to the position at the institution; either entry or modification of student notes; students and parents through Ethereum access the data of institution for the verification of notes in subjects.

By the security provided using blockchain, the information contained in the blocks is encrypted; this information is not altered and has a unique identifier, the Blockchain administrator gives the privileges of a specific block to the required node.

Internal Revenue Service: Users of the organization through Hyperledger permissions store records of tax returns of individuals and companies in the database; this data is available through the web portal of entity; through permission of Ethereum, individuals or companies make their records of the statements and also view the statements in the database.

Smart Contract Functions:

Register Private User: base administrator makes records of persons belonging to the public organization; these users typically interact with the system and are on the Hyperledger network.

Register public user: Update of external persons of the public organization, such as suppliers, citizens, taxpayers, private companies, among others; are on the Ethereum network.

Remove User: User is inactive for access to the database of organization.

Edit User: Performs maintenance on user data; either by errors in the information, as a refresh in your data.

Log event in Hyperledger log: Logs private user movements that occur in the database.

Log event in Ethereum log: Records the movements of the public user that occur in the database.

Validate User: Verification of user access data if it is internal or external in the public organization.

Assign access to the user: Managing detailed control over users to access the system using login credentials.

Update Roles: Maintaining the permissions that the administrator provides to the internal or external user of the public organization.

Assign Role to User: Defining the permissions that the administrator provides to the user of the processes that are deployed.

Validate User Request and Process: Verifying the permissions the user requires to use.

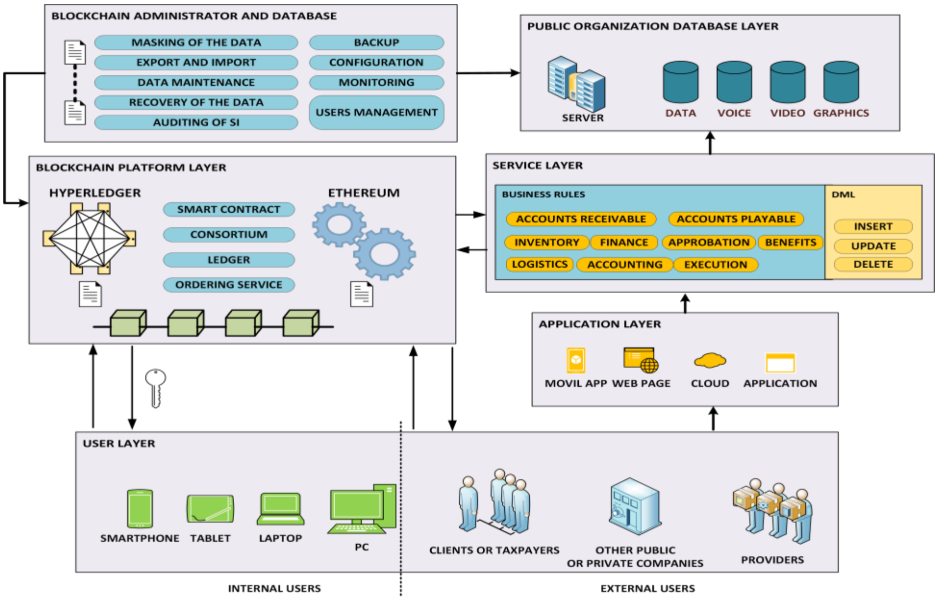

FIGURE 2. Architecture prototype of a database security management on Blockchain for a database in a public organization.

The mathematical livelihood for measuring the average number of connected users in the blockchain system was raised in the formula (4)

$$U_{BC} = \frac{UEthereum}{UHyper} \tag{4}$$

Intermediaries are calculated with the following summary proposed in the formula (5)

$$NoS = \sum_{i=1}^{n} x_i \tag{5}$$

To measure the efficiency of the architecture we have proposed the formula (6)

$$E = 100 - \left(\frac{U_{BC} * NoS}{\sqrt{\operatorname{Re} DB}} \right) \tag{6}$$

In formula (4) variables are used, UEthereum is the number of users outside the public organization, located on Ethereum, UHyper is the number of internal users of the public organization, located in Hyperledger

In the calculation of the formula (5) the Variables Services is determined is the number of services located in the Services layer, App is the number of applications that the organization has, located in the Applications layer and FunctionSC that is the number of functions of the smart contract, located on the blockchain platform, within the sum.

Variables were used to measure the architecture, Ubc is the average number of users using the blockchain system.

ReDB is the number of records in the public database of organization.

Figure 3 presents the simulation in twelve scenarios; the first scenario has 89.95% efficiency with 9975 users, 55 processes and 100916 records in the database; the sixth scenario has 98.98% efficiency with 6364 users, 44 processes and 308729 records in the database; the tenth scenario has 99.50% efficiency with 2385 users, 48 processes and 237229 records in the database.

Testing results from 89.95% to 99.50%, we infer that architecture efficiency is maintained at the same level based on the number of database records.

Figure 4 presents the second simulation that allowed to denote the effectiveness according to the number of users connected, in the first scenario a total of 7064 users were connected to the platform using 47 processes, with an effectiveness of 98.75% and in the last scenario a total of 8385 users connected with 43 processes used with an 97.97% effectiveness were recorded.

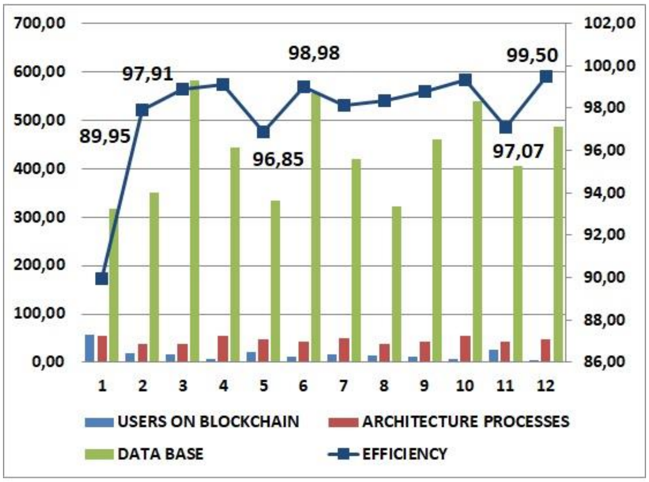

FIGURE 3. **Efficiency analysis of a database security system.**

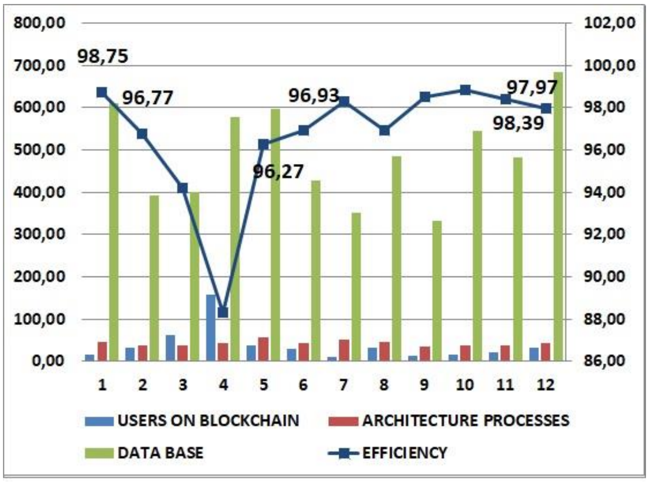

FIGURE 4. **Efficiency analysis of a database security system.**

Figure 5 found several scenarios above 90% efficiency, in the first scenario you will connect 8587 users to the system that used 45 processes with a 97.87 era and the last scenario with 7543 connected users that used 53 processes with a 95.40% era.

Each simulation performed on this model was determined by randomly taken data, this data was assigned in an Excel table according to a range close to reality; the data studied were analyzed through a conventional system used by the entities; each data refers to the number of users, number of processes performed by users in a certain time, the logs that are stored, the number of applications within the system used by users; the users identified for this process are users with Hyperledger and Ethereum system, using the smart contract system; the database of data storage, execution times, use of processes and functions; for the measurement of the efficiency of the architecture were used each of the actors related to this model already exposed above.

Efficiency is given according to the results of the simulations performed by us, the data were entered according to the studies carried out; adopting the above formula (6), the results of the efficiencies were determined.

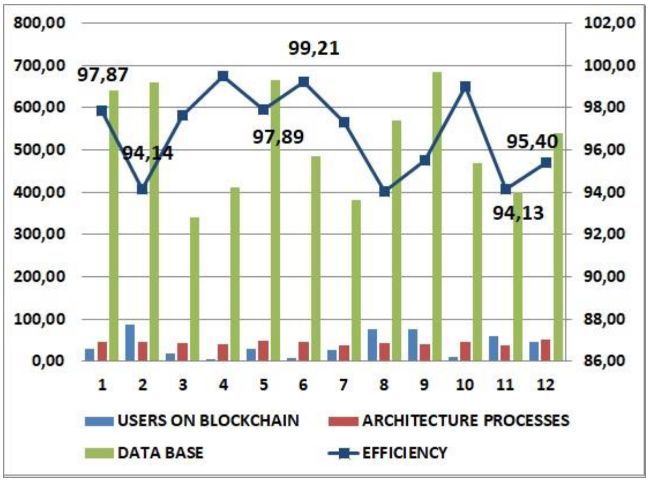

FIGURE 5. **Efficiency analysis of a database security system.**

The values of variables with random values were determined in the simulations; external users of the organization or entity were determined as UEthereum, the range of this variable is between 1000 and 10000 users; internal users of the organization were determined with UHyper and the variable range is between 50 and 500 users; for applications, services and futions were determined with the variables App, Services and FunctionSC are between 10 and 20 programs each; records were determined by the ReportDB variable and the range of values is between 100000 and 500000 records in the database; We form three groups, users on blockchain containing internal and external users, architectural processes containing the number of applications, services and functions of the smart contract; database that contains the square root of the number of records in the DB.

Figure 3 presents the efficiency values with the best effectiveness rate according to the requirements of the architecture; formula (7) calculates the averages of the values of each previously performed simulation:

$$AEf = \sum_{i=1}^{Scenarios} Ef_i \qquad (7)$$

The overall average of architecture is presented in simulated scenarios; for this exercise is 97.74% on average in efficiency, in the second simulation 96.68% efficiency was achieved and the last simulation achieved 96.80% efficiency.

C. ALGORITHM PROTOTYPE OF SECURITY FOR DATABASES

The management of information and application processes in public entities in Latin America are sometimes a problem of execution by users in the system; the users that were handled on the system are users of the entity and external users, each user presented a different type of role; according to the architecture of the previous point and by studying the important factors a door was found to the system that allowed users to enter the system.

The scenario being raised was similar to the architecture design, according to the type of user, the system used its authentication method with encryption for a possible information theft attack; the system compared with the data provided by the user with its database, for access to the system; the role verification process was performed and according to the results obtained, users used the processes; important factors for algorithm performance required actors for each step throughout the process; requests to use processes by users, application response, and information support throughout the process.

The users that intervened in the system according to the architecture model were Ethereum blockchain users and Hyperledger blockchain users; in view of the problems exposed, it was necessary to record the events carried out throughout the process; according to the requirements of the entities a security process was needed for users to have security in the data they provided or searched; the data obtained at the end of each session, was of great importance that I provided a security system that complied with the requirement.

As a study of the above we proposed an algorithm of access to the database on hybrid architecture in a public organization; this algorithm provides management in database security. Figure 6 presents the steps in flowchart techniques.

The mathematical sustenment of the algorithm is the formula (8)

$$LdR=\frac{BCEntries}{TotalEntries}*100\% \tag{8}$$

Here:

LdR is the request payload on the system according to the blockchain entries.

BCEntries is the number of Ethereum or Hyperledger blockchain entries.

TotalEntries is the total number of system entries made by users.

This algorithm handled a user validation system, so accessing the application required permission from the administrator; according to the permissions that the Blockchain administrator provided to the user, internal or external users perform necessary processes on the system; this helps organizations seeking improvement in the data logging system and will depend on their application; the algorithm will complement data security through Blockchain and keep track of permissions, accesses and movements, these remain immutable.

To determine the load of the login request system, the established formula of the number of Hyperledger user entries in the system and also the total number of user input was established; in the simulation we determined a total of 850 entries throughout the system, of the entries made, there were a total of 560 entries of Hyperledger users; calculating determined a request load of 65.88% load on the system.

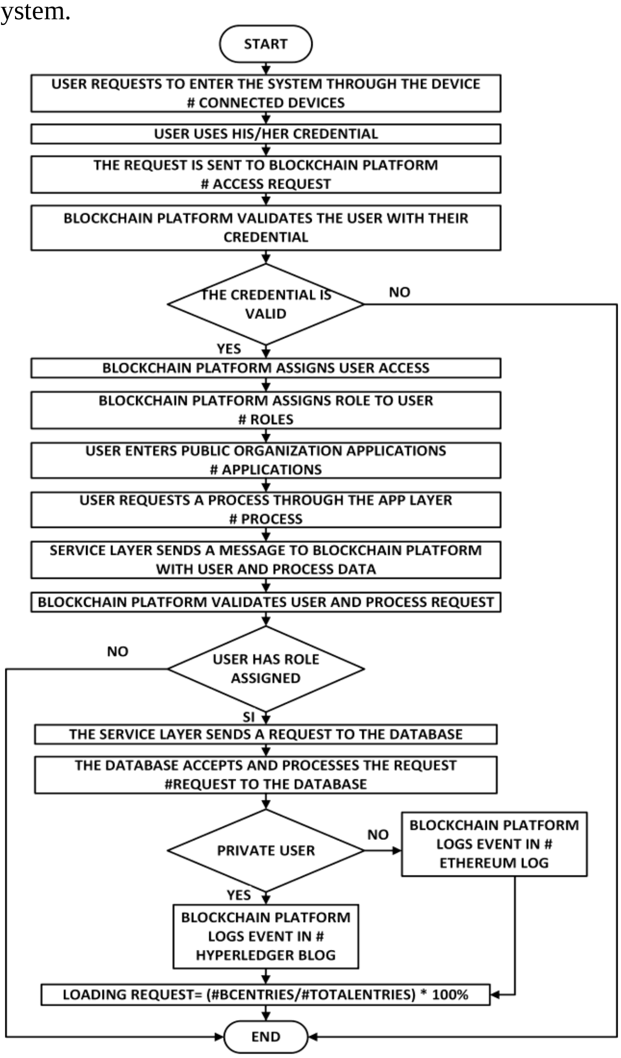
START
USER REQUESTS TO ENTER THE SYSTEM THROUGH THE DEVICE
# CONNECTED DEVICES
USER USES HIS/HER CREDENTIAL
THE REQUEST IS SENT TO BLOCKCHAIN PLATFORM
# ACCESS REQUEST
BLOCKCHAIN PLATFORM VALIDATES THE USER WITH THEIR CREDENTIAL
THE CREDENTIAL IS VALID
NO
YES
BLOCKCHAIN PLATFORM ASSIGNS USER ACCESS
BLOCKCHAIN PLATFORM ASSIGNS ROLE TO USER
# ROLES
USER ENTERS PUBLIC ORGANIZATION APPLICATIONS
# APPLICATIONS
USER REQUESTS A PROCESS THROUGH THE APP LAYER
# PROCESS
SERVICE LAYER SENDS A MESSAGE TO BLOCKCHAIN PLATFORM WITH USER AND PROCESS DATA
BLOCKCHAIN PLATFORM VALIDATES USER AND PROCESS REQUEST
NO
USER HAS ROLE ASSIGNED
SI
THE SERVICE LAYER SENDS A REQUEST TO THE DATABASE
THE DATABASE ACCEPTS AND PROCESSES THE REQUEST
#REQUEST TO THE DATABASE
PRIVATE USER
NO
BLOCKCHAIN PLATFORM LOGS EVENT IN # ETHEREUM LOG
YES
BLOCKCHAIN PLATFORM LOGS EVENT IN # HYPERLEDGER BLOG
LOADING REQUEST= (#BCENTRIES/#TOTALENTRIES) * 100%
END

FIGURE 6. **Algorithm prototype of security for databases.**

This will help the blockchain system administrator the ability to identify the load according to the connected users of the different platforms.

To measure the minimum probability of efficiency of the algorithm we proposed the formula (9)

$$M\,\mathrm{P}=\left(1-\frac{1}{Us*\mathrm{R}\,q}\right)^{\left((Us*\mathrm{R}\,q)-5\right)} \tag{9}$$

Here:

MP is minimum efficiency by the number of connections.

Us is the number of users connected to the architecture.

Rq is the number of requests per user.

U and Rq is the number of transactions performed.

Division is to maximize the probability of efficiency; the power is to get the minimum efficiency of the algorithm; it subtracts 5 because they are 5 layers of the architecture.

In the following cases, simulations were performed to measure the effectiveness of the algorithm used, according to the number of requests that users make to perform a transaction; users involved in the algorithm are identified according to the type of blockchain they use to interact with the system; formula (9) was used in the simulations to identify the probabilities in the efficiency of the algorithm so the results presented below were obtained:

The simulation presented the following scenarios: from 5 to 30000 connected users and a random number of requests, both are on the X axis; the minimum probability of efficiency is on y-axis; for 10 users with 2 requests each, there is 59.05% minimum efficiency shown in Figure 7; for 45 users with 3 requests each, there is 40.44% minimum efficiency shown in Figure 8; for 1000 users with 4 applications each, there is 36.83% minimum efficiency in Figure 9; for 25000 users with 6 requests each, there is 36.79% minimum efficiency; for 30000 users with 3 requests each, there is 36.79% minimum efficiency; this tells us that by increasing the number of users and requests, the efficiency of the algorithm is above 36.01% in the first simulation and 36.79% in the other simulations.

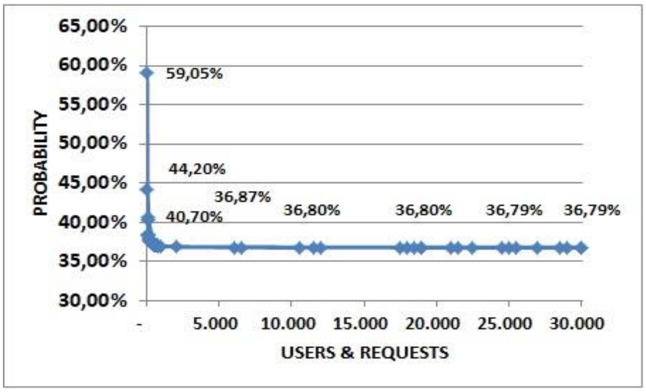

FIGURE 7. First simulation used to measure the efficiency of the security algorithm.

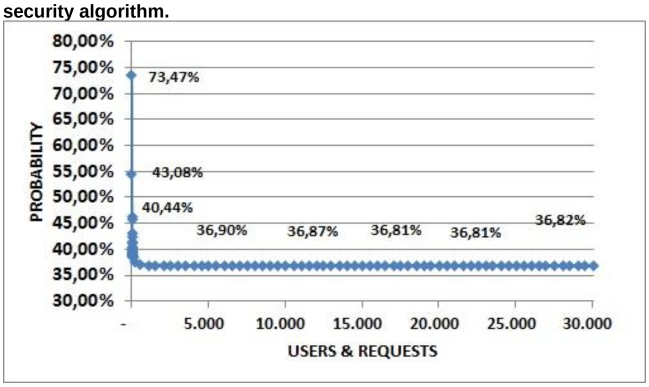

FIGURE 8. Second simulation of the efficiency of the database security algorithm.

D. LOGICAL STRUCTURE OF THE MANAGEMENT SYSTEM ON BLOCKCHAIN

We proposed a security management model for public organizations, this model helped user interaction with the database (Figure 10); blockchain platforms allowed access to different services according to the permissions that users or members of the organization held; using the logical model shows the relationships of the tables, the user table contains the data of external users and users belonging to the organization; the Roles table contains the different roles of a user in the organization and the generic roles of external users; the system table contains the system status; the Applications table contains the means for the user to interact with the service within the system; the encrypted key table contains the keys of system users; the login table contains the data of the created session, the time and date the user enters the system to keep track of the events or interactions.

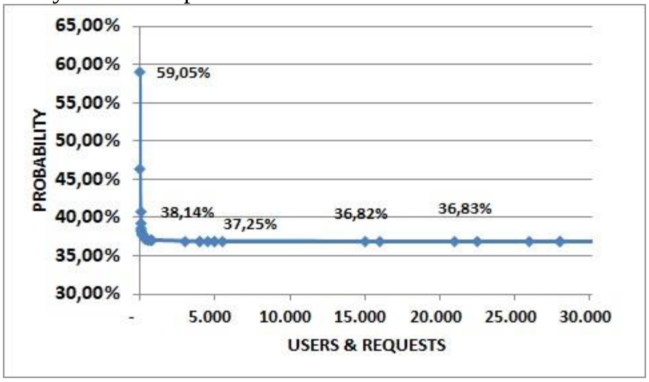

FIGURE 9. Third simulation of the efficiency of the database security algorithm.

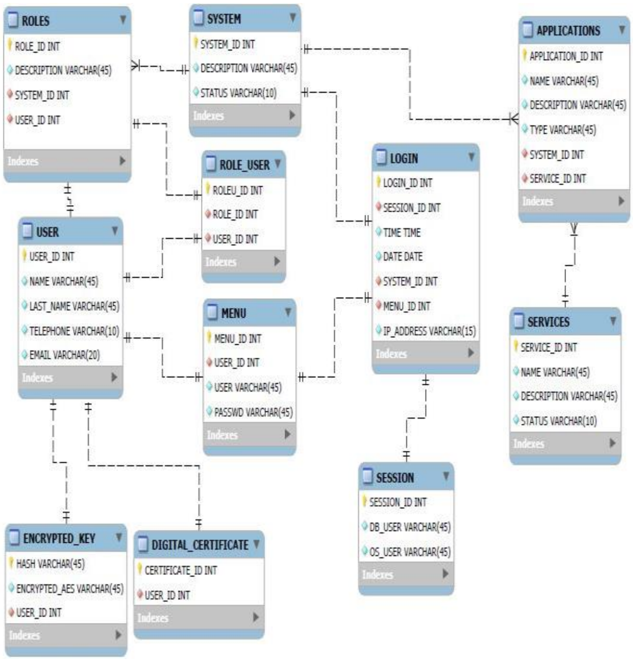

FIGURE 10. Logical structure of the management system on Blockchain.

The mathematical sustenment of the logical structure is applied in formula (10)

$$SysPerf = \frac{DS - DF}{Uc * \sqrt{Up}} * 100\% \qquad (10)$$

Here:

DS is the amount of data interactions the user has with the system.

DF is the number of failed interactions that occur in the system.

Uc is the total number of users connected to the system

Up is the number of processes that users use during all interaction with the system.

Simulation is presented with random inputs to the system, users interact directly with the data entry to the tables or make use of the services and that have system failures.

Figure 11 a simulation consisting of 14 scenarios was presented, users enter the system and in each scenario consists of a certain number of users connected to the system; each user makes the request for the processes covered by the system; each user has a success rate and a failure rate in the instant of interacting with the system; as we see in the graph in the first scenarios we have an efficiency of 48.22% this is the case with the most failures in interaction with the system; in the seventh scenario we have as an efficiency of 86.27% this is the case with the least failures at the instant of performing an interaction with the system; this tells us that according to the permissions that users have, the efficiency of the system was established in optimal conditions with lower failure rate.

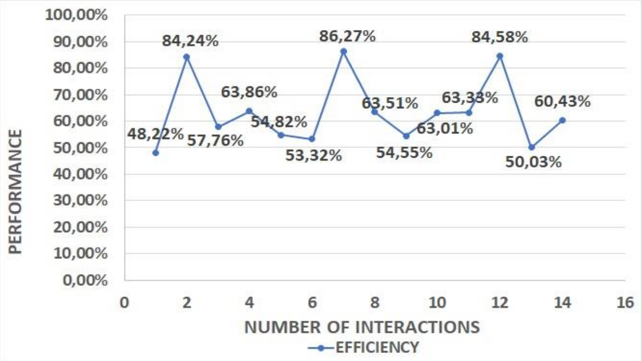

FIGURE 11. First simulation of the performance of the database security management system.

Figure 12 simulation was presented with a medium failure rate around 55%, in the first scenario you can visualize an 85.07% simulation with less failures in interaction with the system; the average in this simulation denotes that there is an effectiveness of between 50.95% to 88.25% at the time the user makes the request for the service; according to the results obtained, users had a failure rate of approximately 50% so the possible factors that intervened to occur the displayed on the graph.

The last simulation performed is shown in Figure 13, users enter the system and make the request to the system processes; the percentage of effectiveness is displayed so that the task is met with the lowest failure rate; in the first scenario we have an efficiency of 86.71% with interaction, using established processes; the last scenario we have an efficiency rate of 66.93% being considered an acceptable efficiency rate compared to the tenth scenario with a rate of 41.59%.

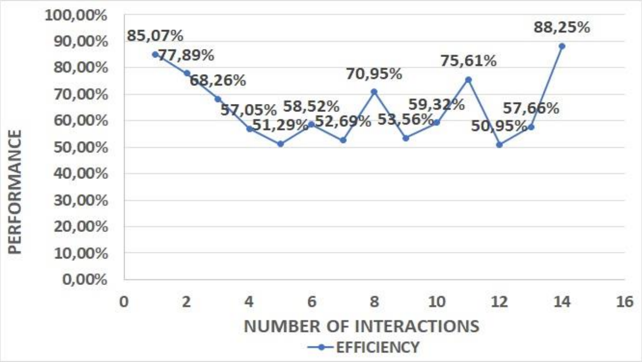

FIGURE 12. Second simulation of database security management system performance.

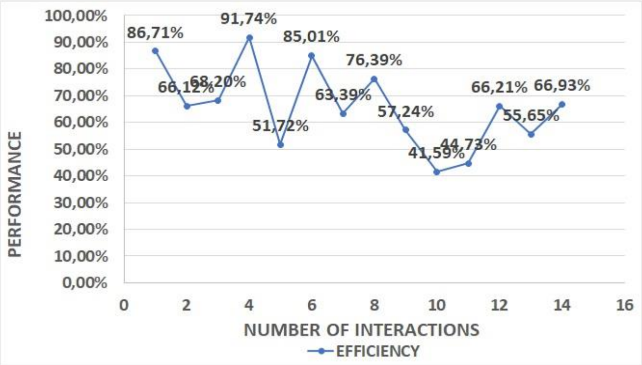

FIGURE 13. Third simulation of database security management system performance.

E. PROTOTYPE TO MITIGATE CYBERNETIC ATTACKS

A prototype was proposed to detect threats on the network; according to the studies carried out in the document, threats were found that may compromise the information of the public entity; Figure 14 depicts a frequent attack on systems.

As a mathematical sustenement to measure the probability of the arrival of an attack on the system is shown in the formula (11)

$$P_A(n) = \frac{(\lambda A)^n e^{-\lambda A}}{n!} \qquad (11)$$

$$\lambda = \frac{W_t}{t}$$

Here:

P_A is the probability of an attack occurring in the system.

λ is the average number of processes used in the system by the user.

n is the number of threats that need to be measured.

Wt is the number of processes used by users.

t is the runtime that delays the process in performing the task.

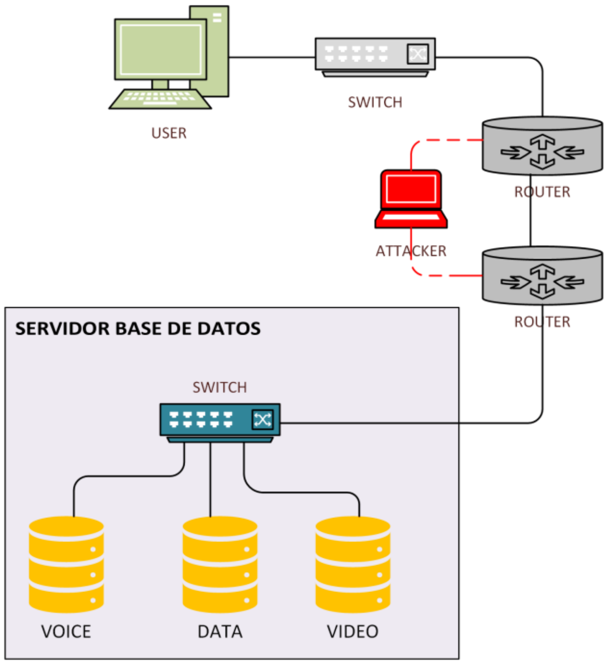

FIGURE 14. Graph representative of a man-in-the-half attack on the database system.

To determine the probability of an attacker performing three attacks entering the system using the man model in the middle, a scenario with 5 processes were performed for two and a half minutes; formula (11) determined a 19.53% chance of receiving an attack on the database system.

With the information received, convergence with the architecture was determined to identify threats in systems that may be affected; security management with information technology that is handled by database system administrators are responsible for mitigating vulnerabilities; applying the results of the different methods can identify errors in the network and apply changes to improve the system of public entities by being a target of attacks by third parties.

IV. DISCUSSION

According to the results obtained by the prototype of the architecture that we have proposed; the interaction of internal or external users, applications and a good management of database security by administrators, ensured the efficiency of the system employed; through blockchain the system allowed security from the first interaction with the system to the storage in the database.

Architectural prototypes and security algorithm ensure application usage in accordance with established permissions; the logical model and evaluation model of a public organization focused on the analysis and management of permissions according to users that interact with the base; being an information exchange model, better data management was achieved in the system by applying blockchain, the prototype to mitigate the attacks and the proposed architecture focused on identifying the communication channels so that they could identify the problems that arise in the system.

In the analysis that we carried out, there were cases of systems that adopted a system similar to that proposed by us as in Table I; a hybrid blockchain management model was applied for the adaptation of the architecture prototype; This made it easier for the administrator to identify and maintain control over users that interact with the system, to have data security.

TABLE I
CYBERSECURITY MODELS

Model	Process	Efficiency%	Ref.
Intrusion detection system	It monitors processes for an intrusion into the system to stop the anomaly.	69.91%	[1]
Packet Sniffing	Packets that traverse the network are detected, and then scanned.	87.49%	[2]
Block network in Hyperledger	They are used for greater data reliability and scalability in the system.	33% - 99%	[3]
Blockchain application in Chinese government	It has a method of managing services to have reliability in data.	Model only	[4]
Hopping mechanism	Authentication data and port are stored by a node that moves randomly in a certain instant of time.	Model only	[5]
Honeypot	It is a resource that determines the different threats and provides how the system is attacked.	Model only	[6]
Risk matrix	It is a model that aims to be able to counteract the risks that arise.	60%	[8]
Anomaly detection	It performs an analysis on the queries that the user performs to obtain patterns of possible anomalies.	Architecture only	[9]
Database System Managed	Users in the system need authorization to be able to manipulate the data.	30% - 40%	[10]
Mechanism Blockchain-based multimode mechanism.	Exchange of information in the business database and better information management.	Architecture only	[11]
Information management system with Blockchain integration.	Companies store their data in blocks to provide confidentiality in transactions.	Architecture only	[13]
Blockchain-based data management platform	It gives solution to the attempt of unauthorized access and makes a record of the activities carried out.	Architecture only	[14]
Data masking	The information in a database is masked to maintain the original appearance.	Algorithm only	[18]
Data storage	Keys are used for secure	Algorithm	[19]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022746, IEEE Access

and recovery method	communication, to access database data.	only	
Hybrid model	Acquires the security provided by a blockchain network with the speed of a centralized database, for better data processing.	Model only	[20]

Table I contains the evaluation of the security models implemented in relation to the revised articles; in some cases the models did not obtain a quantitative measure; while in other cases it obtained the efficiency of some models like Blockchain and this obtained up to 99% effectiveness.

The proposed prototype does not determine the system implementation values, so implementation will depend only on the country that wants to adapt our proposal.

In the article [2] algorithms were used to minimize the arrival of an attack; in the articles [3] and [21] a client-server application was used; in the article [6]a cheat database was used: in the article [7] a contingency plan was used; in the article [8] a risk model was used for information security control; in the article [16] an algorithm was used to detect activity in the system; in the articles [18] and [19] an asymmetric encryption algorithm was used.

According to database security models, it is necessary to implement management for data reliability to public entities systems; in this way the efficiency of the system would provide entities with protection of user interaction with the system of the organization.

Establish risk assessment models, system monitoring and strategies against malicious entries in public organization systems.

V. FUTURE WORKS AND CONCLUSIONS

It was concluded that the prototype of the proposed architecture on a hybrid blockchain model provides an optimal security system for public organizations; according to the architecture simulation, the database has greater effectiveness up to 99.50% in security, this simulation was performed by means of random data based on real situations.

The security assessment prototype provides public organizations with better management of system resources, better control over users interacting with the system, and a study of possible improvements the system may experience.

Public organizations are guaranteed through the security algorithm to have an identification of users according to the permissions provided by the blockchain administrator.

In the future, we proposed the application of database security systems for countries with high rates of cyberattacks in public organizations in Latin America.

ACKNOWLEDGMENT

The authors thank to Salesian Polytechnic University of Ecuador, to the research group of the Guayaquil Headquarters “Computing, Security and Information Technology for a Globalized World” (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt).

REFERENCES

[1] A. Sallam, E. Bertino, S. R. Hussain, D. Landers, R. M. Lefler, and D. Steiner, “DBSAFE - An Anomaly Detection System to Protect Databases From Exfiltration Attempts,” IEEE Syst. J., vol. 11, no. 2, pp. 483–493, 2017, doi: 10.1109/JSYST.2015.2487221.

[2] S. M. T. Toapanta, J. D. L. Cobeña, and L. E. M. Gallegos, “Analysis of cyberattacks in public organizations in Latin America,” Adv. Sci. Technol. Eng. Syst., vol. 5, no. 2, pp. 116–125, 2020, doi: 10.25046/aj050215.

[3] S. M. T. Toapanta, F. G. M. Quimi, M. G. T. Espinoza, and L. E. M. Gallegos, “Proposal of a model to apply hyperledger in digital identity solutions in a public organization of Ecuador,” Proc. 3rd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2019, pp. 21–28, 2019, doi: 10.1109/WorldS4.2019.8903981.

[4] H. Hou, “The application of blockchain technology in E-government in China,” 2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017, pp. 4–7, 2017, doi: 10.1109/ICCCN.2017.8038519.

[5] Z. Cui, J. Zeng, C. Wu, and S. Zhang, “Design and implementation of a new database security model based on hopping mechanism,” Proc. Int. Conf. Anti-Counterfeiting, Secur. Identification, ASID, vol. 2016-Febru, no. 13, pp. 1–5, 2016, doi: 10.1109/ICASID.2015.7405649.

[6] M. Wegerer and S. Tjoa, “Defeating the database adversary using deception - A MySQL database honeypot,” Proc. - 2016 Int. Conf. Softw. Secur. Assur. ICSSA 2016, pp. 6–10, 2017, doi: 10.1109/ICSSA.2016.8.

[7] S. M. T. Toapanta, I. N. C. Ochoa, R. A. N. Sanchez, and L. E. G. Mafla, “Impact on administrative processes by cyberattacks in a public organization of Ecuador,” Proc. 3rd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2019, pp. 270–274, 2019, doi: 10.1109/WorldS4.2019.8903967.

[8] S. M. T. Toapanta, L. B. Peñafiel, and L. E. M. Gallegos, “Prototype to mitigate the risks of the integrity of cyberattack information in electoral processes in Latin America,” ACM Int. Conf. Proceeding Ser., no. December, pp. 111–118, 2019, doi: 10.1145/3375900.3375915.

[9] J. H. Roh, S. H. Lee, and S. Kim, “Anomaly detection of access patterns in database,” Int. Conf. ICT Converg. 2015 Innov. Towar. IoT, 5G, Smart Media Era, ICTC 2015, pp. 1112–1115, 2015, doi: 10.1109/ICTC.2015.7354751.

[10] A. A. Shastri and P. N. Chatur, “Efficient and effective security model for database specially designed to avoid internal threats,” 2015 Int. Conf. Smart Technol. Manag. Comput. Commun. Control. Energy Mater. ICSTM 2015 - Proc., no. May, pp. 165–167, 2015, doi: 10.1109/ICSTM.2015.7225407.

[11] X. Zhang et al., “Blockchain-based safety management system for the grain supply chain,” IEEE Access, vol. 8, pp. 36398–36410, 2020, doi: 10.1109/ACCESS.2020.2975415.

[12] W. Zheng, Z. Zheng, P. Li, and R. Chen, “NutBaaS : A Blockchain-as-a-Service Platform,” vol. 7, 2019.

[13] K. C. Chan, X. Zhou, R. Gururajan, X. Zhou, M. Ally, and M. Gardiner, “Integration of Blockchains with Management Information Systems,” Proc. 2019 Int. Conf. Mechatronics, Robot. Syst. Eng. MoRSE 2019, no. December, pp. 157–162, 2019, doi: 10.1109/MoRSE48060.2019.8998694.

[14] H. Cui, Z. Chen, Y. Xi, H. Chen, and J. Hao, “IoT data management and lineage traceability: A blockchain-based solution,” 2019 IEEE/CIC Int. Conf. Commun. Work. China, ICCC Work. 2019, pp. 239–244, 2019, doi: 10.1109/ICCChinaW.2019.8849969.

[15] J. W. Pan, Z. Min, C. Ping, and W. G. Xu, “A Lightweight Vulnerability Scanning and Security Enhanced System for Oracle Database,” Proc. 2019 IEEE 4th Adv. Inf. Technol.

Electron. Autom. Control Conf. IAEAC 2019, no. Iaeac, pp. 1699–1702, 2019, doi: 10.1109/IAEAC47372.2019.8997534.

[16] H. Mazzawi et al., “Anomaly detection in large databases using behavioral patterning,” Proc. - Int. Conf. Data Eng., pp. 1140–1149, 2017, doi: 10.1109/ICDE.2017.158.

[17] U. Albalawi, “Countermeasure of Statistical Inference in Database Security,” Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018, pp. 2044–2047, 2019, doi: 10.1109/BigData.2018.8622241.

[18] F. You, C. Zhang, Y. Cao, H. Gong, C. Zhang, and J. Liao, “Data Masking System Based on Ink Technology,” Proc. - 2018 5th Int. Conf. Inf. Sci. Control Eng. ICISCE 2018, no. 1, pp. 176–180, 2019, doi: 10.1109/ICISCE.2018.00046.

[19] T. M. Zaw, M. Thant, and S. V. Bezzateev, “Database Security with AES Encryption, Elliptic Curve Encryption and Signature,” 2019 Wave Electron. its Appl. Inf. Telecommun. Syst. WECONF 2019, no. 978, 2019, doi: 10.1109/WECONF.2019.8840125.

[20] E. Safak, A. Furkan, and T. Erol, “Hybrid Database Design Combination of Blockchain and Central Database,” 3rd Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2019 - Proc., 2019, doi: 10.1109/ISMSIT.2019.8932763.

[21] J. C. Odirichukwu and P. O. Asagba, “Security concept in web database development and administration-A review perspective,” 2017 IEEE 3rd Int. Conf. Electro-Technology Natl. Dev. NIGERCON 2017, vol. 2018-Janua, pp. 383–391, 2018, doi: 10.1109/NIGERCON.2017.8281910.

[22] M. Kantarcioglu and F. Shaon, “Securing big data in the age of AI,” Proc. - 1st IEEE Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. TPS-ISA 2019, pp. 218–220, 2019, doi: 10.1109/TPS-ISA48467.2019.00035.

[23] C. Egbunike and S. Rajendran, “The implementation of negative database as a security technique on a generic database system,” Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2017, 2017, doi: 10.1109/ICCPCT.2017.8074342.

[24] Y. Chen and W. W. Chu, “Protection of database security via collaborative inference detection,” IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1013–1027, 2008, doi: 10.1109/TKDE.2007.190642.

[25] O. Elaswad and C. D. Jensen, “Identity management for e-government Libya as a case study,” 2016 Inf. Secur. South Africa - Proc. 2016 ISSA Conf., pp. 106–113, 2016, doi: 10.1109/ISSA.2016.7802936.

[26] H. Chen, D. Bao, H. Gao, and J. Cheng, “A Security evaluation and certification management database based on ISO/IEC standards,” Proc. - 12th Int. Conf. Comput. Intell. Secur. CIS 2016, pp. 249–253, 2017, doi: 10.1109/CIS.2016.63.

[27] O. Cinar, R. H. Guncer, and A. Yazici, “Database Security in Private Database Clouds,” ICISS 2016 - 2016 Int. Conf. Inf. Sci. Secur., 2017, doi: 10.1109/ICISSEC.2016.7885847.

[28] T. Y. Win, H. Tianfield, and Q. Mair, “Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing,” IEEE Trans. Big Data, vol. 4, no. 1, pp. 11–25, 2017, doi: 10.1109/tbdata.2017.2715335.

[29] M. Zhang, P. Martin, W. Powley, and J. Chen, “Workload management in database management system: A taxonomy (Extended Abstract),” Proc. - IEEE 34th Int. Conf. Data Eng. ICDE 2018, vol. 30, no. 7, pp. 1823–1824, 2018, doi: 10.1109/ICDE.2018.00269.

[30] S. El Haddouti and M. D. Ech-Cherif El Kettani, “Analysis of identity management systems using blockchain technology,” Proc. - 2019 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2019, 2019, doi: 10.1109/COMMNET.2019.8742375.

[31] E. Chukwu and L. Garg, “A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations,” IEEE Access, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[32] K. Zhou, S. Member, J. Ren, and S. Member, “PassBio : Privacy-Preserving User-Centric Biometric Authentication,” vol. 13, no. 12, pp. 3050–3063, 2018.

[33] A. Detti, G. Rossi, and N. B. Melazzi, “Exploiting Information-Centric Networking to Federate Spatial Databases,” IEEE Access, vol. 7, pp. 165248–165261, 2019, doi: 10.1109/ACCESS.2019.2953043.

[34] J. Preciozzi et al., “Fingerprint Biometrics From Newborn to Adult: A Study From a National Identity Database System,” IEEE Trans. Biometrics, Behav. Identity Sci., vol. 2, no. 1, pp. 68–79, 2020, doi: 10.1109/tbiom.2019.2962188.

[35] P. Y. Chen, J. X. Wu, C. M. Li, C. L. Kuo, N. S. Pai, and C. H. Lin, “Medical Image Infosecurity Using Hash Transformation and Optimization-Based Controller in a Health Information System: Case Study in Breast Elastography and X-Ray Image,” IEEE Access, vol. 8, pp. 61340–61354, 2020, doi: 10.1109/ACCESS.2020.2983428.

[36] L. Yao, J. Lu, J. Liu, D. Wang, and B. Meng, “A Secure and Efficient Distributed Storage Scheme SAONT-RS Based on an Improved AONT and Erasure Coding,” IEEE Access, vol. 6, pp. 55126–55138, 2018, doi: 10.1109/ACCESS.2018.2872749.

[37] S. Wang, X. Wang, and Y. Zhang, “A Secure Cloud Storage Framework With Access Control Based on Blockchain,” IEEE Access, vol. 7, pp. 112713–112725, 2019, doi: 10.1109/access.2019.2929205.

[38] K. Hao, J. Xin, Z. Wang, K. Cao, and G. Wang, “Blockchain-based outsourced storage schema in untrusted environment,” IEEE Access, vol. 7, pp. 122707–122721, 2019, doi: 10.1109/ACCESS.2019.2938578.

[39] H. Y. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee, and S. K. Lo, “Analysis of data management in blockchain-based systems: From architecture to governance,” IEEE Access, vol. 7, pp. 186091–186107, 2019, doi: 10.1109/ACCESS.2019.2961404.

[40] N. B. Truong, K. Sun, S. Member, G. M. Lee, and S. Member, “GDPR-Compliant Personal Data Management: A Blockchain-Based Solution,” vol. 15, no. March, pp. 1–13, 2019.

[41] M. Kim, H. T. Lee, S. Ling, S. Q. Ren, B. H. M. Tan, and H. Wang, “Search Condition-Hiding Query Evaluation on Encrypted Databases,” IEEE Access, vol. 7, pp. 161283–161295, 2019, doi: 10.1109/ACCESS.2019.2951695.

[42] Y. Xu and Y. Huang, “Segment blockchain: A size reduced storage mechanism for blockchain,” IEEE Access, vol. 8, pp. 17434–17441, 2020, doi: 10.1109/ACCESS.2020.2966464.

[43] X. Xie, C. Ren, Y. Fu, J. Xu, and J. Guo, “SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN,” IEEE Access, vol. 7, pp. 151475–151481, 2019, doi: 10.1109/ACCESS.2019.2947527.

[44] H. Mei, Z. Gao, Z. Guo, M. Zhao, and J. Yang, “Storage Mechanism Optimization in Blockchain System Based on Residual Number System,” IEEE Access, vol. 7, pp. 114539–114546, 2019, doi: 10.1109/access.2019.2934092.

[45] R. Gyorodi, M. I. Pavel, C. Gyorodi, and D. Zmaranda, “Performance of OnPrem Versus Azure SQL Server: A Case Study,” IEEE Access, vol. 7, pp. 15894–15902, 2019, doi: 10.1109/ACCESS.2019.2893333.

[46] W. Yuan, “Fair Data Transactions across Private Databases,” IEEE Access, vol. 8, pp. 53720–53732, 2020, doi: 10.1109/ACCESS.2020.2979813.

[47] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, “A blockchain privacy protection scheme based on ring signature,” IEEE Access, vol. 8, pp. 76765–76772, 2020, doi: 10.1109/ACCESS.2020.2987831.

[48] M. Binjubeir, A. A. Ahmed, M. A. Bin Ismail, A. S. Sadiq, and M. Khurram Khan, “Comprehensive survey on big data privacy protection,” IEEE Access, vol. 8, pp. 20067–20079, 2020, doi: 10.1109/ACCESS.2019.2962368.

[49] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, “A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure,” IEEE Access, vol. 6, pp. 25167–25177, 2018, doi: 10.1109/ACCESS.2018.2817560.

[50] X. Li and H. Li, “A Visual Analysis of Research on Information Security Risk by Using CiteSpace,” IEEE Access, vol. 6, pp. 63243–63257, 2018, doi: 10.1109/ACCESS.2018.2873696.

[51] S. Yaseen et al., “Improved Generalization for Secure Data Publishing,” IEEE Access, vol. 6, pp. 27156–27165, 2018, doi: 10.1109/ACCESS.2018.2828398.

[52] M. Monshizadeh, V. Khatri, B. G. Atli, R. Kantola, and Z. Yan, “Performance Evaluation of a Combined Anomaly Detection Platform,” IEEE Access, vol. 7, pp. 100964–100978, 2019, doi: 10.1109/access.2019.2930832.

[53] Y. Wang, Y. Shen, C. Su, J. Ma, L. Liu, and X. Dong, “CryptSQLite: SQLite with High Data Security,” IEEE Trans. Comput., vol. 69, no. 5, pp. 666–678, 2020, doi: 10.1109/TC.2019.2963303.

[54] H. A. Lee et al., “An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study,” J. Med. Internet Res., vol. 22, no. 6, p. e16748, 2020, doi: 10.2196/16748.

[55] Internet Crime Complaint Center, “FBI 2019 Internet Crime Report,” *Fed. Bur. Investig. - Internet Crime Complain. Cent.*, pp. 1–28, 2019, [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf.

SEGUNDO M. TOAPANTA is professor on of Computer Science at the Salesian Polytechnic University, Guayaquil, Ecuador. Coordinator research group: “Computing, Security and Information Technology for a Globalized World” “CSITGW”. He is an evaluator and accredited researcher of the Senescyt with No. REG-INV. 16-01530. He is a Computer Science Engineer. He obtained his MSc. In ICT at the National Polytechnic School. He completed his doctoral stay at the Department of Information Technology and Communications of the Polytechnic University of Cartagena UPCT, Spain. He obtained the degree of PhD. In Information Technology at the University of Guadalajara, Mexico. He has published 84 scientific articles in journals and conference proceedings in database EEE Xplore, ACM Digital, ScienceDirect, Springer, among others indexed in Scopus, EI Compendex, Scimago, Web of Science, He has worked in public and private institutions at an operational, tactical and strategic level in Ecuador, Colombia and Peru. His research areas are: Strategic alignment of ICT, Distributed systems, Networks, Security and cryptography, Cybersecurity, Cyberbullying, Blockchain technologies and applications

OMAR A. ESCALANTE was born in Guayaquil, Ecuador in 1994. He is a student at the Salesian Polytechnic University, Guayaquil, Ecuador. He studied at the Domingo Comin missionary school and obtained the degree of bachelor in computer electronics, Guayaquil, Ecuador in 2012. He has worked in the private sector, serving as SAP maintenance analyst at Owens Illinois, Guayaquil, Ecuador in 2018. He has worked at Ales Industries serving as an IT Support Assistant, Guayaquil, Ecuador in 2019. He has worked as an IT Support Analyst at Tiendec, Guayaquil, Ecuador in 2019 until 2020. His area of interest is networks, computer security and infrastructure.

LUIS E. MAFLA is a professor in the Informatics and Computer Science Department, at Escuela Politecnica Nacional in Quito, Ecuador. He got his MSc and PhD degree es in computer science at Purdue University, West Lafayette. Dr. Mafla has published in IEEE Computer, USENIX Journal on Computing Systems, Computer Networks and ISDN Systems, and proceedings of international IEEE, ACM and Springer conferences. Dr. Mafla has been a visiting professor at the University of Florida and worked for the Food and Agriculture Organization of the United Nations in Rome and Accra. He has been a consultant in the FAO and projects funded by the Interamerican Development Bank. His research interests include distributed systems, cryptography, networking, and blockchain technologies and applications.

ROCIO M. 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.