Abstract: We analyzed the problems of security of the information of the civil registries and identification at world level that are considered strategic. The objective is to adopt the appropriate security protocols in a conceptual model in the identity management for the Civil Registry of Ecuador. In this phase, the appropriate security protocols were determined in a Conceptual Model in Identity Management with Authentication, Authorization and Auditing (AAA). We used the deductive method and exploratory research to define the appropriate security protocols to be adopted in the identity model: IPSec, DNSsec, Radius, SSL, TLS, IEEE 802.1X EAP, Set. It was a prototype of the location of the security protocols adopted in the logical design of the technological infrastructure considering the conceptual model for Identity, Authentication, Authorization, and Audit management. It was concluded that the adopted protocols are appropriate for a distributed database and should have a direct relationship with the algorithms, which allows vulnerability and risk mitigation taking into account confidentiality, integrity and availability (CIA).

Keywords: Authentication, Authorization, Audit, Identity Models, Security Protocols.

I. INTRODUCTION

Civil registry information security issues at the global level are considered strategic; Considering that based on this information the authorities as presidents, mayors, governors define public policies at a strategic, tactical and operational level to fulfill their management for which they were elected; The analysis of the current situation of Las TICS in Ecuador[1]. How do Tecnologías de Información y Comunicación Impactan la Optimización de los Procesos para el Desarrollo Local [2]. (Analysis of gender and ethnicity variables in Ecuador issued by the Inter-American Development Bank (IDB)). (The Glossary for Civil Registries and Identification issued by (IDB) is considered). (The antecedents determine the problem of information security that seeks a solution integral at the National Plan for Good Living in Ecuador (PNBV 2013-2017) Objective 11). A comprehensive solution to information security problems that include theoretical contributions, management models, evaluation and audit models.

The civil registry of Ecuador is integrated to the National System of Public Data that is empowered to provide information to people from different public and private organizations such as: Internal Revenue Service, National Electoral Council, National Secretariat of Education, Ministries, and International Organizations, authorized by the competent authorities. The civil registry information is...
inconsistent with integrity and confidentiality issues defined in the reference article [3]. It is considered the information of the analyzes to define the identity management reasons why it is important for security [4]. By considering strategic: (The National Assembly of Ecuador in the Official Register Supplement 684 of February 4, 2016 creates the Organic Law of Management of Identity and Civil Data in Article 6 Lit.2 says: Promote, in coordination with the Secretariat of Education and other public and private institutions, scientific and technological research to strengthen the management of identity data and civil registry). The importance of security protocols to be applied in an identity model [5]. Reference is made to a conceptual model to mitigate the security of the database[6].

Why is it necessary to apply the appropriate security protocols for a Conceptual Model in Identity Management for the Civil Registry of Ecuador?

To mitigate the vulnerabilities and risks of information in the civil registry database.

The objective is to adopt the appropriate security protocols in a conceptual model in the identity management for the Civil Registry of Ecuador.

The paper considered for this research are:

Las TICS en el Ecuador[1], Tecnologías de Información y Comunicación Impactan la Optimización de los Procesos para el Desarrollo Local[2], Security analysis of civil registry database of Ecuador[3], Analysis to define management of identities access control of security processes for the registration civil from Ecuador[4], Analysis of suitable security protocols for apply a model of identity in the civil registry of Ecuador[5], Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador[6], Auction Model Using RR Approach for SLA Based Resource Provisioning in Multi- Cloud Environment[7], Secure Inter Hop Verification with Onion Protocol Implementation for Reliable Routing In Wireless Networks[8], Implementation of IPSec protocol[9], Protocol Modifications for the DNS Security Extensions[10], Analysis, implementation and extensions of RADIUS protocol[11], Accelerating SSL with GPUs[12], Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)[13], Extensible Authentication Protocol (EAP) Key Management Framework[14], When private set intersection meets big data: An efficient and scalable protocol[15], Diameter Base Protocol The[16], Security for the internet of things: A survey of existing protocols and open research issues[17].

The deductive method is used with exploratory research to determine the appropriate security protocols to be adopted in a conceptual model of identity management; the defined security protocols are: Ipsec, DNSsec, Radius, SSL, TLS, IEEE 802.1X EAP, Set.

It was concluded that the adopted protocols are appropriate for a distributed database and should have a direct relationship with the algorithms, which allows vulnerability and risk mitigation taking into account confidentiality, integrity and availability (CIA).

II. METHODS

The deductive method was used in the exploratory research to determine in the first instance the appropriate security protocols that are adopted in the logical design of the technological infrastructure of the civil registry of Ecuador; to mitigate vulnerabilities, risk information in a distributed database
that provides confidentiality, integrity and availability. In the first phase we analyzed the paper published by the author that are directly related to the research topic; for continuing with the initial project proposed "Algorithms and security protocols for the Civil Registry of Ecuador". With the antecedents exposed the following articles of different authors related directly to the security protocols such as: Cloud Computing. The resources available in the cloud can be shared by several users and allow reallocation with each demand. So, there has always been focus on best techniques to provision the available resources in the Cloud. Different kinds of clouds Environment: Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud: These types of environments must provide security to mitigate the vulnerability of information through different protocols and security algorithms[7]. Mobile Adhoc Network security (Manet) is complicated due to topology and vulnerabilities in wireless networks. The standard protocol with the algorithms (AES) and the route-referral algorithm are important. It is proposed that the routing be in each network[8]. IPSec protocol defines a final use for traffic to guarantee the authenticity and confidentiality of data packets. IPsec is in the network layer. NLSP relied on the SP3 protocol that was published by NIST, but designed by the National Security Administration's (NSA) Secure Data Network System project. IPSec is a protocol defined by technicians who work in the engineering of internet. IPSec continues authentication encryption and key management routines that allow the mitigation of authentication, authorization and auditing of data on the Internet through public IP networks[9]. DNS security is resource records and protocol modifications that provide authentication and data source integrity to the DNS. In this article we can observe the modifications of the DNSSEC protocol. In addition, the concept of a zone of signatures, along with the requirements to serve and solve using the DNSSec protocol, is defined. This is a technique for solving both DNS and resource level errors [10]. RADIUS (remote authentication dial in the user service) is an authentication, authorization and accounting protocol used in Lan, Many Wan network. It has certain vulnerabilities because of poor implementation as a security protocol [11]. SL/TLS is a standard protocol used on the Internet for secure communications. SSL is a robust protocol but is largely limited to centralizing critical domains in security. This protocol has a low adoption rate in view that requires robust servers. SSL proxy can be designed and deployed for cryptographic downloads to GPUs. The evaluation indicators define that the implementation of GUPU for cryptographic operations in AES and HMAC achieves high performance[12]. In the last decade there are several significant attacks to TLS (Transport Layer Security), these attacks have been detected that have been made in mode of operation. These files contain the summary of these attacks, this deduction is made in order to motivate generic and specific recommendations of the TLS protocol [13]. EAP in an authentication protocol, defined in RFC 3748, for access to the network. This article defines the hierarchy of the EAP protocol that provides for the transport and use of keys and parameters generated by authentication algorithms such as EAP: Which in information security is known as "Methods". It also provides a security analysis in the different operating system platforms; Describing the key management rules and procedures noted in RFC 4962 [14]. Storage at the corporate and reserved level has created new trends for prototype design that provide information privacy considering that the flow of information must be fast, efficient for the performance of modern applications, and how to scale without problems when The data that is protected is large [15]. Diameter is a security protocol designed to provide Authentication, Authorization, and Accounting (AAA) for all applications that connect through the IP protocol locally. In this article defines the format of messages, form of transport, an error report; A security audit using the Diameter protocol [16]. The Internet project of things has a future vision on the internet so that the users, systems, technologies and all the devices that today possess a capacity for the detection and action interact for the benefit of the users. Internet architecture and IP-based communication protocols play an important role in the connectivity of all devices and applications for proper operation. The internet of things is the union of different teams through a communication protocol to provide better services to users in a globalized environment [17].
A. Strength of security protocols

All security protocols operate on most of the OSI layer but each is specialized for Identification, Authenticity, Authorization and Auditing (IAAA). Next, a table is elaborated with the detail being made each one of the safety protocols adopted.

| Security protocols for adoption | Identity | Authentication | Authorization | Audit |
|--------------------------------|----------|----------------|---------------|-------|
| IPsec                          | X        | X              | X             | X     |
| DNSSec                         | X        | X              | X             | X     |
| Radius                         | X        | X              | X             | X     |
| SSL                            | X        | X              | X             | X     |
| TLS                            | X        | X              | X             | X     |
| IEEE 802.1X y EAP              | X        | X              | X             | X     |
| SET                            | X        | X              | X             | X     |
| Diameter                       | X        | X              | X             | X     |

All security protocols listed have (IAAA); But the strength of each of them in the table is defined with red color

B. Security protocol flow

Identity, Authentication, Audit Authorization (IAAA) flow throughout the network to mitigate the vulnerability and risk of information to have Confidentiality, Integrity and Availability (CIA). The distributed main database and backups were protected with security protocols.

III. RESULT

This research results in a prototype of the location of the security protocols adopted in the logical design of the technological infrastructure considering the conceptual model for Identity, Authentication, Authorization, and Audit management.

Fig. 1. Prototype adoption of security protocols in logical design
IV. DISCUSSION

We considered the security protocols that have the greatest strength for Identification, Authentication, Authorization and Auditing at the level of the entire network flow; more than the TCP/IP protocol which is the standard defined by the OSI model for connectivity at the level of all operating system platforms and networking equipment. Other security protocols can be considered in the implementation to mitigate information with confidentiality, integrity and availability (CIA); will depend on the security policies of the organization.

V. FUTURE WORD AND CONCLUSION

Carry out the analysis of the appropriate security algorithms and integrate the security protocols that are defined prior to the implementation of the integral project that is Algorithms and security protocols for the civil registry of Ecuador; as an integral solution to information security problems that include theoretical contributions, management models, evaluation models and auditing.

It was concluded that the adopted protocols are appropriate for a distributed database and should have a direct relationship with the algorithms, allowing to mitigate vulnerabilities and risks taking into account confidentiality, integrity and availability (CIA).

ACKNOWLEDGMENT

The authors thank the CUCEA of Universidad de Guadalajara, Jalisco, México, Program IT PhD Information Technologies, Universidad Politécnica Salesiana del Ecuador and Secretaria de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

REFERENCES

[1] Moisés Toapanta, “Las TICS en el Ecuador,” Rev. Científica Int. Strateg. Sección Tecnol. la Inf. Vol. 1, Numer. I ISSN No. 1390-9568. Guayaquil - Ecuador, vol. 1, pp. 1–10, 2016.
[2] R. M. Moisés Toapanta, “Tecnologías de Información y Comunicación Impactan la Optimización de los Procesos para el Desarrollo Local,” in I Congreso Internacional Investigación en Desarrollo Local y Emprendimiento Socioeconómico Sustentable y Sostenible. Sección “Tecnologías de Información” ISBN 978-9942-1471-1. Guayaquil - Ecuador, 2015, pp. 310–323.
[3] P. D. Student, S. Moisés, T. Toapanta, P. D. Luis, and E. Mafla, “Security analysis of civil registry database of Ecuador,” Int. Conf. Electr. Electron. Optim. Tech. - 2016, pp. 1024–1029, 2016.
[4] P. Segundo, M. Toapanta, P. D. Luis, and E. Mafla, “Analysis to define management of identities access control of security processes for the registration civil from Ecuador,” in 2016 IEEE International Smart Cities Conference (ISC2), 2016, pp. 80–84.
[5] A. O. Moisés Toapanta, Enrique Mafla, “Analysis of suitable security protocols for apply a model of identity in the civil registry of Ecuador,” Abstr. Emerg. Trends Sci. Res. Tracks “Computer Sci. Commun. ISSN. 2415-6914. Indexado en ISI Thomson Reuters, Scopus. Dubai - Emiratos Arab., 2016.
[6] M. Toapanta, E. Mafla, and J. Orizaga, “Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador,” Mater. Today Proceedings. ISSN No. 2214-7853 Index. Scopus CPCI (Thomson Reuters, Web Sci., 2016.
[7] N. Rizvi, P. Pranav, B. Raj, and S. Paul, “Auction Model Using RR Approach for SLA Based Resource Provisioning in Multi-Cloud Environment,” vol. 8, no. 2, pp. 774–784, 2016.
[8] N. Ravi and P. Jeyanthi, “Secure Inter Hop Verification with Onion Protocol Implementation for Reliable Routing In Wireless Networks,” vol. 8, no. 1, pp. 183–190, 2016.
[9] H. Dhali, D. Dhali, S. Batra, and P. Rani, “Implementation of IPSec protocol,” Proc. - 2012 2nd Int. Conf. Adv. Comput. Commun. Technol. ACCT 2012., pp. 176–181, 2011.
[10] B. Soediono, “Protocol Modifications for the DNS Security Extensions,” rfc, vol. 53, p. 160, 2005.
[11] J. Feng, “Analysis, implementation and extensions of RADIUS protocol,” in Proceedings - 2009 International Conference on Networking and Digital Society, ICNDS 2009, 2009, vol. 1, pp. 154–157.
[12] K. Jang, S. S. Han, S. Moon, and K. Park, “Accelerating SSL with GPUs,” ACM SIGCOMM Comput. Commun. Rev., vol. 41, no. 1, p. 135, 2011.

[13] Y. Sheffer, R. Holz, and P. Saint-Andre, “Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS),” RFC 7457, pp. 1–13, 2015.

[14] B. Aboba, D. Simon, and P. Eronen, “When private set intersection meets big data: An efficient and scalable protocol,” 2008.

[15] C. Dong, L. Chen, and Z. Wen, “When private set intersection meets big data: An efficient and scalable protocol,” CCS, pp. 1–29, 2013.

[16] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn, “Diameter Base Protocol The,” Internet Eng. Task Force, pp. 1–151, 2012.

[17] J. S. S. Jorge Granjal, Edmundo Monteiro, “Security for the internet of things: A survey of existing protocols and open research issues,” IEEE Commun. Surv. Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.