Risk analysis and prevention in computer security in institutional servers, a systematic review of the literature

Angel Namo-Ochoa[1], Eduardo Portilla-Cosar[1], Fernando Sierra-Liñan[2], Michael Cabanillas-Carbonell[3]
[1]Facultad de Ingeniería y Negocios, Universidad Privada Norbert Wiener, Lima, Perú
[2]Facultad de Ingeniería, Universidad Privada del Norte, Lima, Perú
[3]Vicerrectorado de Investigación, Universidad Privada Norbert Wiener, Lima, Perú

Article Info

Article history:

Received Feb 26, 2023
Revised Jun 22, 2023
Accepted Nov 14, 2023

Keywords:

Attacks
Risk
Security
Servers
Systematic review

ABSTRACT

In recent years, computer attacks on the server infrastructure in organizations have been increasing, and the pandemic of covid-19 and remote work have been the main causes for this massive wave of large-scale attacks, small businesses are especially vulnerable because to optimizing resources they leave aside the cyber security in their network infrastructure. The present research is a systematic review that compiles 58 articles where policies, techniques, and infrastructure for the prevention of threats in enterprise servers have been implemented and raised, these articles have been collected from major databases such as IEEE Xplore, SAGE, Science Direct, Scopus, and IOP Publishing. The results show that one of the most effective methods in preventing communications between institutional servers is public key infrastructure/SSL-TLS encryption. Most research claims that it is the most effective method as it provides a central certifier and manages the certificates for the servers allowing each of the modules or attachments within the infrastructure to identify and validate other members and to proceed with the encryption of network traffic, Finally, a security implementation model is proposed.

Corresponding Author:

Michael Cabanillas-Carbonell
Vicerrectorado de Investigación, Universidad Norbert Wiener
Lima, Perú
Email: mcabanillas@ieee.org

1. INTRODUCTION

The wave of sophisticated attacks on an organization's cybersecurity creates threats, risks, and challenges, raising national and international awareness of cybersecurity implications [1]. Risk is the possibility of an undesired event occurring due to uncertainty about information security [2], [3]. Risk management identifies, assesses, and prioritizes risks [4]. Servers are becoming important to today's Internet infrastructure [5]. Most web server architectures in use today are designed to improve server performance by using a single server. The author mentions that information security is the process of establishing and observing a set of strategies, policies, techniques, rules, guidelines, practices and procedures to prevent, protect and safeguard against damage, evidence, or theft of an organization's computer resources and to manage the risk by ensuring as much as possible the proper and uninterrupted operation of those resources [6]. Therefore, it is intended to know the use of digital technologies to facilitate the analysis and prevent the risks of information security in institutional servers, this prevention allows to keep the risks on computer resources to a minimum [7].

2. METHOD

The 2020 Prism methodology replaces the 2009 statement and includes a new presentation guide that reflects advances in methods of research identification, selection, evaluation, and synthesis [8]. A systematic review of the scientific literature will be used for the development of the article. The questions posed are the following:

RQ1: what security methods allow for efficient server protection?
RQ2: which security technologies can be used to ensure the security of the organization's servers?
RQ3: which are the most frequent risks according to their origin and type?

In order to answer the research questions, a search for published articles in the main database platforms such as IEEE Xplore, EBSCO, Science Direct, Scopus, and IOP Publishing. Database platforms such as IEEE Xplore, EBSCO, Science Direct, Scopus, and IOP Publishing. The following keywords were considered in the research search: (ALL ("defense technologies") AND ALL ("information security" OR “server security") AND ("information security") OR ("computer risks"). Figure 1 shows the collection of articles from each database respectively. For the development of the systematic review, the following aspects and inclusion and exclusion criteria were considered in Table 1. Figure 2 shows the flowchart of the item selection process following the Prisma statement.

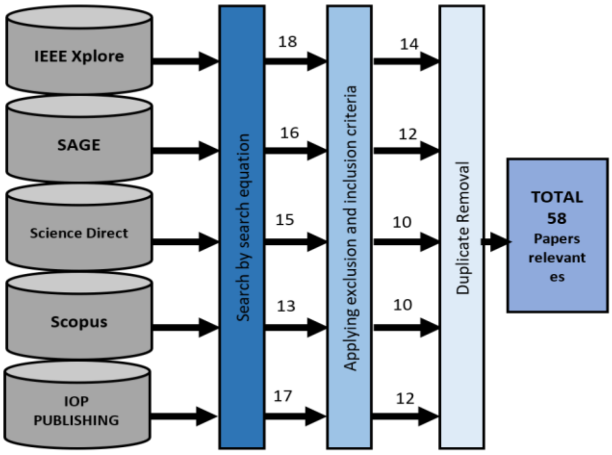


Figure 1. Item inclusion graph

Table 1. Exclusion and inclusion criteria table

		Criteria
Inclusion	I01	Articles related to information technology.
	I02	Articles related to Information security.
	I03	Articles related to information security analysis.
	I04	Articles related to information risks.
	I05	Articles related to IT risk forecasting.
Exclusion	E01	Articles not related to computer servers.
	E02	Articles not oriented to the institutional sector
	E03	Articles related to information security, but oriented to companies.

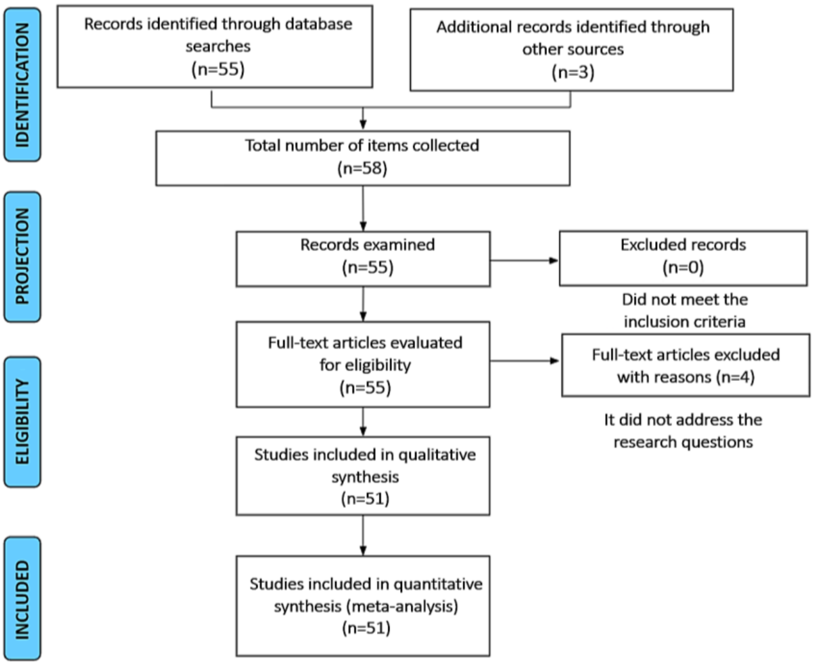

IDENTIFICATION
PROJECTION
ELIGIBILITY
INCLUDED
Records identified through database searches (n=55)
Additional records identified through other sources (n=3)
Total number of items collected (n=58)
Records examined (n=55)
Excluded records (n=0)
Did not meet the inclusion criteria
Full-text articles evaluated for eligibility (n=55)
Full-text articles excluded with reasons (n=4)
It did not address the research questions
Studies included in qualitative synthesis (n=51)
Studies included in quantitative synthesis (meta-analysis) (n=51)

Figure 2. Document inclusion and exclusion flowchart

3. RESULTS

Fifty-eight articles were analyzed from the aforementioned databases, following the search equation. In the review of articles, 3 were excluded according to the exclusion criteria, and 4 did not contribute to answering the research questions. Finally, 51 articles were obtained for the systematic review. Figure 2 shows the Prisma flow chart in the sequence of article collection. Figure 3 shows the number of articles found in the database. Figure 4 shows the number of articles published per month and the database. Figure 5 shows the number of articles published by continent. Figure 6 shows the number of selected items grouped by database and category. Figure 7 shows the relationship between the origin (internal-external) and types of risk (business-process-technical). Figure 8 shows the number of selected articles published by country.

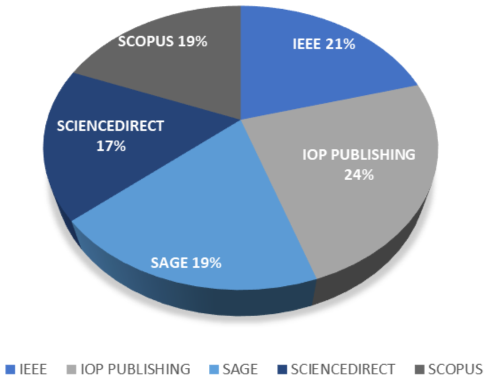


Figure 3. Articles by the database

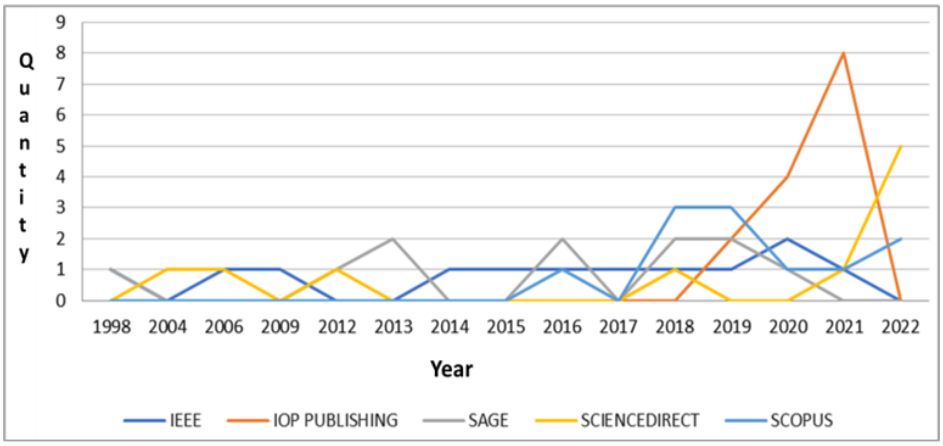
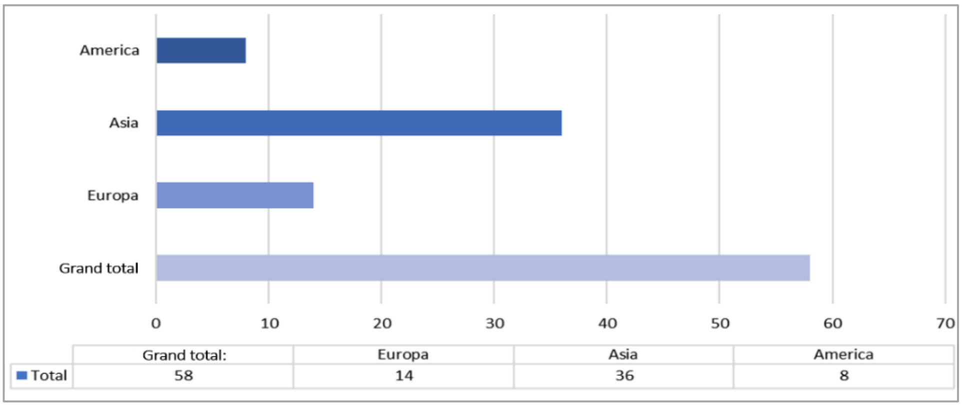


Figure 4. Articles by year and database



	Grand total:	Europa	Asia	America
■ Total	58	14	36	8

Figure 5. Articles by continents

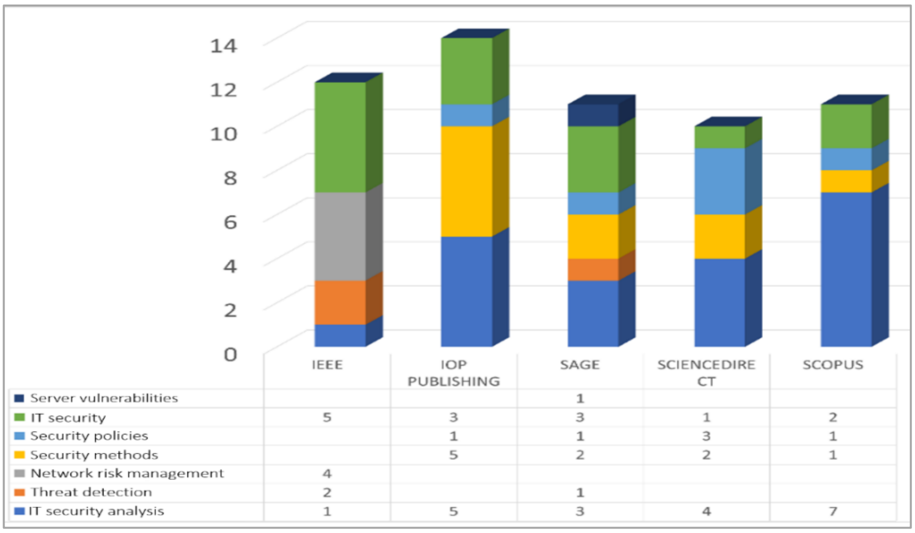


Figure 6. Articles by database and category

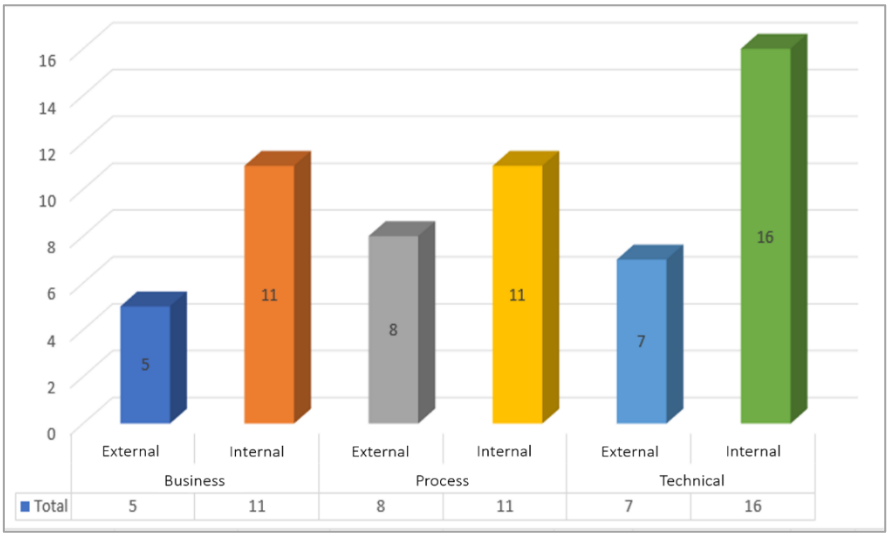


Figure 7. Articles by type of risk and risk factors

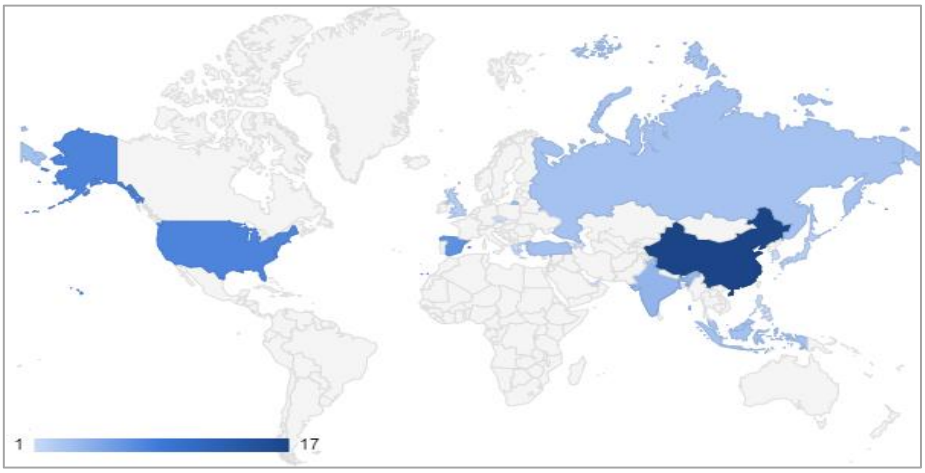
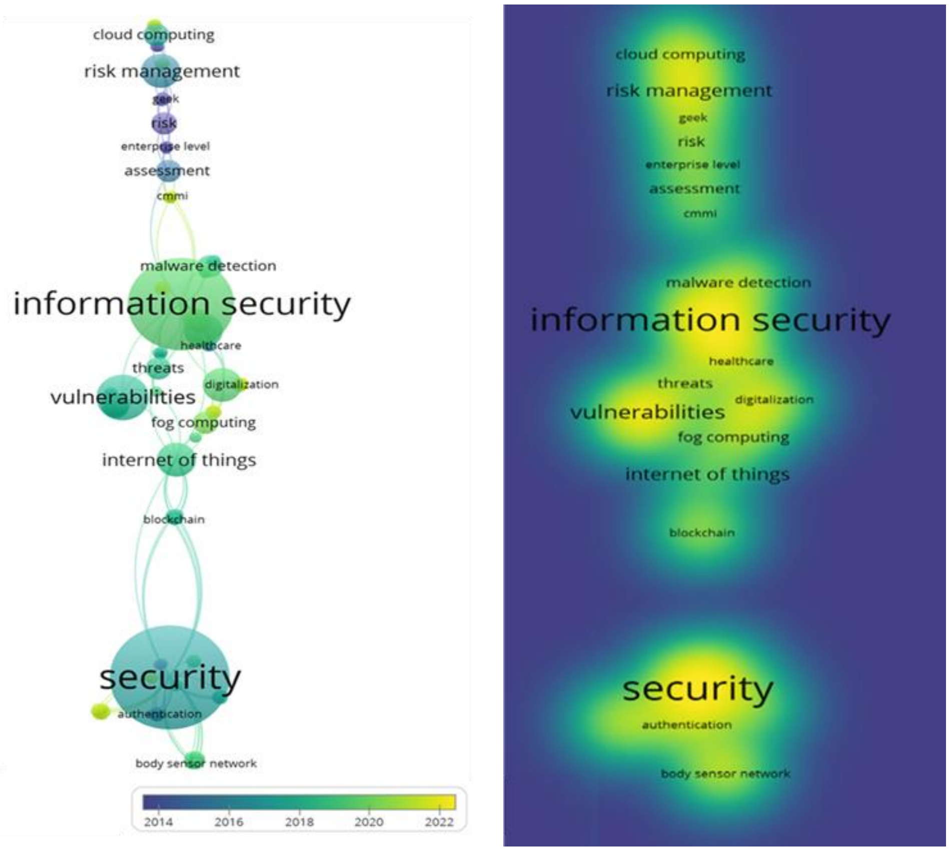


Figure 8. Articles by country

Figure 9 produced with VOSviewer. VOSviewer is a software tool for analyzing and visualizing scientific literature developed by Nees Jan van Eck and Ludo Waltman from the Center for Research in Science and Technology (CWTS) at Leiden University [9]. It can be seen in Figure 9(a) the history in years of the keywords with the most hits, as well as in Figure 9(b) the heat map where the words: computer security, security vulnerabilities, risk management and malware detection are highlighted, which aims to answer the research questions with the topics of the articles.



(a) (b)

Figure 9. Network visualization graph; (a) co-occurrence grouped in clusters and (b) heat map

Biometrics is a science that uses statistical and mathematical procedures in all documents related to scientific subjects and the authors who produce them. This is done to perform a scientific analysis of performance. To this end, it uses the laws of biometrics, which are based on conventional statistical behavior, which has been manifesting the various elements that constitute science over time. The mechanisms used to evaluate aspects of this phenomenon are the so-called biometric indicators, an evaluation that provides information on the outcome of scientific activity according to some of its manifestations.

For this bibliometric analysis, we used RStudio with Bibliometrix, obtaining, as a result, Figure 10, which shows the word cloud collected from the keywords of the selected articles, and Figure 11, which shows the percentage of occurrence of each word, highlighting "security of data" and "network security". Table 2 shows the classification of articles according to the results obtained. Table 3 shows the classification of articles according to the technologies and methods used. Table 4 shows the classification of articles according to categories and topics of functionality. Table 5 shows the classification of articles according to types of risks and origin.

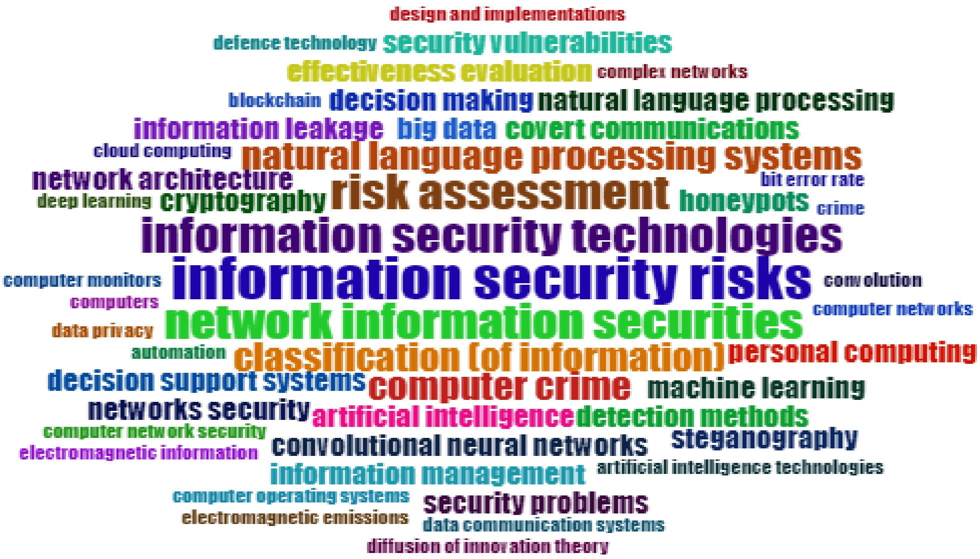


Figure 10. Word cloud

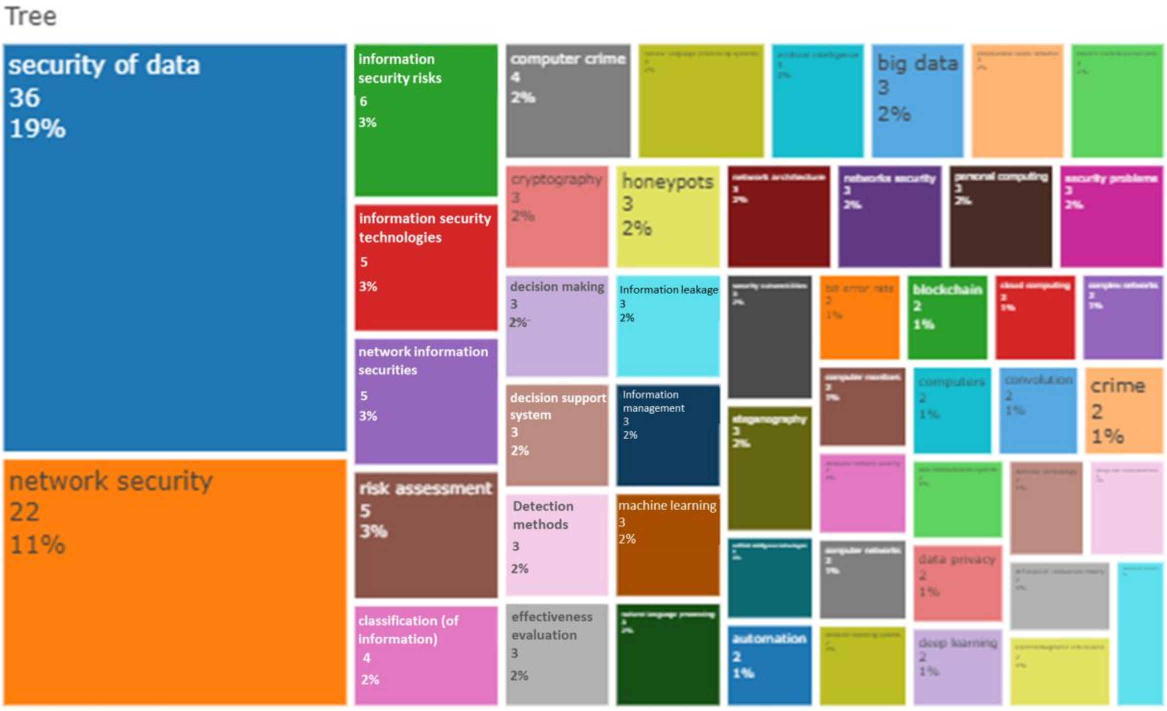


Figure 11. Tree map

Table 2. Classification of articles according to the results obtained

Category	Ref.
IT security analysis	[9]-[27]
Threat detection	[28]-[31]
Network risk management	[2], [32]-[34]
Security methods	[5], [35]-[44]
Security policies	[45]-[50]
IT Security	[1], [51]-[62]
Server vulnerabilities	[63], [64]

Table 3. Classification of articles according to methods and technologies

Methods and technologies	Ref.
SSH key implementation	[13], [14]
Public key infrastructure and SSL/TLS encryption	[20], [21], [27], [28], [34], [43], [51], [54]
Audits of deployed services	[37], [38]
Implementation of VPN and private networks	[20], [21]
Firewall insertion	[26], [27]
Computer auditing and intrusion detection systems (IDS).	[24]-[27], [43]
Isolated execution and testing environments	[9], [22], [23]

Table 4. Classification of items according to categories and topics of functionality

Themes and funcionality	Ref.
These articles argue that the identification of IT resources, their vulnerabilities and the threats to which they are exposed, and their probability and impact, in order to determine the appropriate control measures to accept, reduce, transfer or prevent the risk.	[9]-[27]
These articles argue that the search for external actors or malicious intruders in the network cannot be detected by automated security systems. This analysis can be performed with varying degrees of automation or completely manually. in general.	[28]-[30]
This article argues the use of alternatives to manage the risks to which IT resources may be exposed as part of the organization's processes. This means a well-defined structure with full control and implementation through feasible and effective actions.	[2], [32]-[34]
These articles argue that the use of computer security technology and activities is aimed at ensuring the integrity, availability, and security of data stored in a digital environment.	[5], [35]-[43]
These articles argue that the use of technology and security policies and implementation as well as the responsible use of the organization's resources must be part of the systems implemented for proper management and legal compliance.	[44]-[49]
This article argues that the use of digital technologies and cybersecurity strategies prevent unauthorized access to an organization's resources, such as computers, networks, and data. It maintains the integrity and secrecy of confidential information and blocks access by experienced hackers.	[1], [50]-[62]
These articles argue that server security is as important as network security because they often contain large amounts of important organizational information.	[63]

Table 5. Classification of items according to types of risks and origin

Type of risk	Origin of risk	Ref.
Business	External	[13], [22] [34], [37], [60]
	Internal	[2], [5], [11], [20], [24], [26], [27], [52], [53], [55], [59]
Process	External	[9], [10] [15], [19], [26]-[29], [35], [48]
	Internal	[18], [23], [32], [38], [43], [49], [50] [63]
Technical	External	[1], [39], [40], [44], [46], [54], [61]
	Internal	[13], [14], [16], [17], [21], [30], [33], [41], [42], [45], [47], [51], [56]-[58], [62]

4. DISCUSSION

This systematic review of the scientific literature aims to answer the questions posed:

RQ1. Which security methods allow to carry efficient protection for servers?

According to Table 3, it can be observed that the most used technologies that allow carrying efficient protection for servers are public key infrastructure and SSL/TLS encryption. Semerdzhiev *et al.* [22] mentions that SSH keys can be used for server authentication. This allows us to understand the security that this technology has because the user maintains a private key which is kept securely as a secret on the other hand the public key can be used by different users without restriction. According to Figure 7, it can be determined that the articles that are similar to the research topic use public key infrastructure technology and SSL/TLS encryption. This result gives us to know which technologies are the most used to ensure the protection of servers. Wang *et al.* [23] mentions that a security method that allows the efficient protection of servers is to use active collection and passive collection technologies of devices. With this technology, it will be possible to effectively identify the state of the devices in order to detect their behavior. According to Table 1, the categories of articles are determined in relation to the research topic, these use the technology of "IT security analysis". The result shows that this category is the most recommended for use in the security of institutional servers.

RQ2. What security technologies can be used to ensure the security of the organization's servers?

According to Figure 7, it can be determined that the articles that have similarities to the research topic use IT security analysis technology. This result shows us which technologies are the most used to ensure the protection of servers. Wang *et al.* [23] mentions that SMTP/MYSQL/RDP/DNS/HTTP protocols guarantee the security of servers since they prevent brute force attacks such as ransomware, network attacks, worms, and Trojans. On the other hand, the study [59] mentions that different approaches can be taken to

secure the network and servers. IDS technologies in conjunction with a firewall can detect threats that further ensure the security of the organization's servers because it can detect malicious packets coming from network traffic in time. According to Table 1, it can be seen that the categories of the articles related to the topic in question use the "public key infrastructure and ssl/tls encryption" (the server interconnects the business services and the availability of information) and "computer auditing and IDS". The result indicates that these technologies are the most frequently used in the security of organizational servers. Table 2 shows the functionalities and characteristics of the aforementioned categories using "IT auditing and IDS".
RQ3: What are the most frequent risks according to their origin and type?

According to Figure 7, it can be seen that the risks with the highest number are technical and the origin is internal. It can also be seen in the graph that the origin of the risks comes from internal factors of the institution. On the other hand, it can be identified that the technical risks can considerably affect the institutional servers, this information will allow us to take preventive and corrective measures to avoid a malfunction of the servers. According to Table 3, we can determine the categories of the types and origins of computer risks based on the articles reviewed, this allows us to see their effects can be detrimental, therefore, it is advisable to plan control measures. The study [37] mentions the risk of server outages, which are mainly caused by denial-of-service attacks or DdoS attacks, which are considered more frequent due to the fact that over the years new technologies have emerged and there has been a considerable increase in attacks, putting information security at risk. According to the author in his study [65], he mentions that the most frequent risks come from internal factors due to bad data manipulation, as the servers are constantly under constant risk and highly vulnerable and these are mainly the points for external factors such as attackers to develop different mechanisms to vulnerate and expose the information.

5. PROPOSITION

As an application proposal, we recommend an implementation that includes aspects such as SSH keys, public key infrastructure, and SSL-TLS encryption to prevent threats and negative impacts such as loss of reputation, information theft, paralysis of communications, and availability of information, as show in Figures 12 and 13. The implementation of this technology makes sense when the company is growing since it requires a great economic and management effort. Initially, a certificate authority and certificate manager are needed for the servers, which allows each of the entities integrated into the infrastructure to encrypt traffic and identify users, thus preventing a server spoofing attack used by attackers to intercept traffic. During the implementation period, the use of a VPN is recommended to secure communications until the SSL infrastructure is operational.

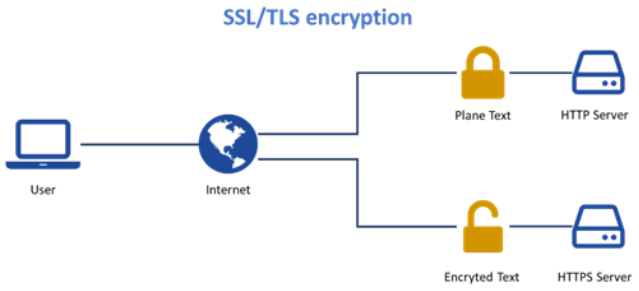


Figure 12. SSL/TLS encryption model graph

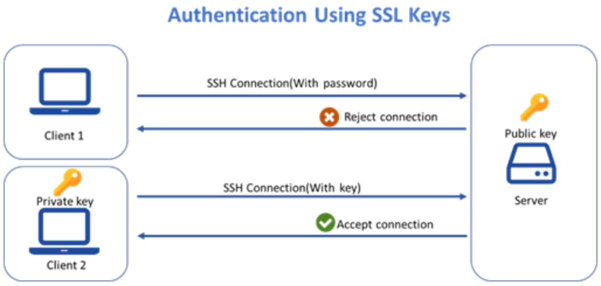


Figure 13. SSL/TLS encryption model graph

6. RELATED TASK

In this systematic review, 58 articles were selected for the identification of techniques and methods in the prevention of computer risks in institutional servers, as well as the security techniques with the best effectiveness according to the results of other research, such as the most used methods and the largest number of researches according to the type of method, countries, and continents. It coincides with the applied implementation [34] of SSL Keys, where it is specified that all connections to the server are made by using public and private keys, dispensing with passwords, its implementation allowed for mitigating server simulation attacks and dictionary and brute force attacks. We agree with the studies [27] in identifying the public key infrastructure and SSL/TLS encryption since they argue that the use of this computer security technology is aimed at ensuring the integrity, availability, and security of data stored in a digital environment. Also, in the study [28] where the use of firewalls and VPN networks where communications are private and can be mapped and monitored, only the servers that have been designed for connections with customers will be the only ones exposed on the public internet, leaving the servers of the internal network protected. Those systematic review researches conducted focus on server risk prevention by focusing on techniques based on the use of SSH keys, and periodic computer audit applications published between the year (2014 to 2022).

7. CONCLUSION

After the systematic review of the scientific literature of 58 articles related to the research topic, it is concluded that: the most susceptible risk factors are those originating internally due to poor data management, as servers are exposed to constant and highly vulnerable risks. The methods or techniques that allow reducing and preventing risks in institutional servers are the methods and technologies associated with the "Implementation of SSL technologies and VPN private networks". In such a way, the research articles' analysts validate the effectiveness of the most used methods and tools. The data obtained from this systematic review can help future research on the most effective technologies and methods for preventing computer risks on servers.

REFERENCES

[1] B. I. Lamarca, "Cybersecurity Risk Assessment of the University of Northern Philippines using PRISM Approach," *IOP Conference Series: Materials Science and Engineering*, vol. 769, no. 1, p. 012066, Feb. 2020, doi: 10.1088/1757-899X/769/1/012066.

[2] B. K. Alese, O. Oyebade, O. A. Festus, O. Iyare, and A. F. Thompson, "Evaluation of information security risks using hybrid assessment model," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, IEEE, Dec. 2014, pp. 387–395, doi: 10.1109/ICITST.2014.7038843.

[3] R. K. B. A. Malviya and A. Sinhal, "A Review of Secure data in the Clouds," *International Journal of Ethics in Engineering & Management Education*, vol. 5, no. 7, pp. 1–3, 2018.

[4] S. M. V. Bharti and A. Sinhal, "Security Enhancement & Risk Minimization Using Key Encryption," *International Journal of Ethics in Engineering & Management Education*, vol. 5, no. 7, pp. 1–14, 2018.

[5] M. Idhom, R. Alit, and A. Fauzi, "Implementation of Web Server Security Against Denial of Service (DoS) Attacks," *IOP Conference Series: Materials Science and Engineering*, vol. 1125, no. 1, p. 12037, May 2021, doi: 10.1088/1757-899x/1125/1/012037.

[6] J. V. M., "Preservación documental digital y seguridad informática," *Investigación Bibliotecológica. Archivonomía, Bibliotecología e Información*, vol. 24, no. 50, Nov. 2010, doi: 10.22201/iibi.0187358xp.2010.50.21416.

[7] V. A. Avdeev, O. A. Avdeeva, V. V. Smirnova, I. M. Rassolov, and M. A. Khvatova, "Improvement of Information Technology and Its Impact on Information Security," *International Journal of Emerging Technology and Advanced Engineering*, vol. 11, no. 11, pp. 15–21, Nov. 2021, doi: 10.46338/ijetae1121_02.

[8] M. J. Page *et al.*, "Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas," *Revista Española de Cardiología*, vol. 74, no. 9, pp. 790–799, Sep. 2021, doi: 10.1016/j.recesp.2021.06.016.

[9] L. Chen, X. Xie, Y. Xu, and D. Xia, "Security analysis and design of a uniform identity authentication system," in *2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, IEEE, Aug. 2009, doi: 10.1109/icasid.2009.5276931.

[10] R. Ismail and A. N. Zainab, "Assessing the status of library information systems security," *Journal of Librarianship and Information Science*, vol. 45, no. 3, pp. 232–247, Mar. 2013, doi: 10.1177/0961000613477676.

[11] T. D. Mai, "Research on Internet of Things security architecture based on fog computing," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, p. 155014771988816, Nov. 2019, doi: 10.1177/1550147719888166.

[12] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control*, vol. 52, no. 5–6, pp. 338–353, Apr. 2019, doi: 10.1177/0020294019837991.

[13] H. Chen, "Intelligence and security informatics: information systems perspective," *Decision Support Systems*, vol. 41, no. 3, pp. 555–559, Mar. 2006, doi: 10.1016/j.dss.2004.06.003.

[14] F. Karlsson, E. Kolkowska, and J. Petersson, "Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis," *Computers & Security*, vol. 114, p. 102578, Mar. 2022, doi: 10.1016/j.cose.2021.102578.

[15] D. Polverini and P. Tosoratti, "Towards a metric for the energy efficiency of computer servers," *Computer Standards & Interfaces*, vol. 55, pp. 116–125, Jan. 2018, doi: 10.1016/j.csi.2017.06.003.

[16] A. S. Auliani and Candiwan, "Information Security Assessment On Court Tracking Information System: A Case Study from Mataram District Court," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, Dec. 2021, doi: 10.1109/uemcon53757.2021.9666617.

[17] D. Tripathi, A. K. Tripathi, L. K. Singh, and A. Chaturvedi, "Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of NPP," *Annals of Nuclear Energy*, vol. 168, p. 108863, Apr. 2022, doi: 10.1016/j.anucene.2021.108863.

[18] H. D. J.s Parada, O. L. R. Bohórquez, and J. F. P. González, "Scheme for the integration of the evaluation of computer security for the recognition phase. Case study: Company in the Colombian accounting sector," in *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)*, IEEE, Oct. 2017, doi: 10.1109/coniiti.2017.8273359.

[19] W. Yustanti, A. Qoiriah, R. Bisma, and A. Prihanto, "An analysis of Indonesia's information security index: a case study in a public university," *IOP Conference Series: Materials Science and Engineering*, vol. 296, p. 12038, Jan. 2018, doi: 10.1088/1757-899x/296/1/012038.

[20] C. Flores, C. Flores, T. Guasco, and J. León-Acurio, "A Diagnosis of Threat Vulnerability and Risk as It Relates to the Use of Social Media Sites When Utilized by Adolescent Students Enrolled at the Urban Center of Canton Cañar," in *Technology Trends*, Springer International Publishing, 2017, pp. 199–214, doi: 10.1007/978-3-319-72727-1_15.

[21] B. N. Akilotu, Z. Kadiroglu, and A. Sengur, "Information Security and Related Machine Learning Applications," in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, IEEE, Nov. 2019, doi: 10.1109/ubmyk48245.2019.8965484.

[22] K. G. A. Semerdzhiev, D. Dimitrov, N. Angelova, P. Armyanov, and T. Trifonov, "Performing computer science examinations in a fully online environment," in *The 14-th conference on Information Systems and Grid Technologies*, Sofia, Bulgaria, pp. 9–21.

[23] S. Wang, L. Zhang, J. Zhang, Y. Tang, and Y. Liang, "Research on Information System Risk Analysis and Security Situation Assessment Method," *Journal of Physics: Conference Series*, vol. 1792, no. 1, p. 12047, Feb. 2021, doi: 10.1088/1742-6596/1792/1/012047.

[24] A. S. Dina and D. Manivannan, "Intrusion detection based on Machine Learning techniques in computer networks," *Internet of Things*, vol. 16, p. 100462, Dec. 2021, doi: 10.1016/J.IOT.2021.100462.

[25] D. Zhou, "Research on the Security Strategy and Technology of Information Resource Network of Chinese Academy Library," *Journal of Physics: Conference Series*, vol. 1550, no. 3, p. 32037, May 2020, doi: 10.1088/1742-6596/1550/3/032037.

[26] L. Zhu, Z. Ma, H. Huang, and M. Yan, "Research on Cybersecurity Risk Prevention and Control of New Infrastructure," *Journal of Physics: Conference Series*, vol. 1856, no. 1, p. 12034, Apr. 2021, doi: 10.1088/1742-6596/1856/1/012034.

[27] Y. Li, R. Liu, X. Liu, H. Li, and Q. Sun, "Research on Information Security Risk Analysis and Prevention Technology of Network Communication Based on Cloud Computing Algorithm," *Journal of Physics: Conference Series*, vol. 1982, no. 1, p. 12129, Jul. 2021, doi: 10.1088/1742-6596/1982/1/012129.

[28] M. S. Makarova and A. A. Maksutov, "Methods of Detecting and Neutralizing Potential DHCP Rogue Servers," in *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, IEEE, Jan. 2021, doi: 10.1109/elconrus51938.2021.9396106.

[29] N. M. Babu and G. Murali, "Malware detection for multi cloud servers using intermediate monitoring server," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, IEEE, Aug. 2017, doi: 10.1109/icecds.2017.8390135.

[30] Y. Cho and G. Qu, "Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 205920, Aug. 2013, doi: 10.1155/2013/205920.

[31] A. J. Altamemi, A. Abdulhassan, and N. T. Obeis, "DDoS attack detection in software defined networking controller using machine learning techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 5, pp. 2836–2844, Oct. 2022, doi: 10.11591/eei.v11i5.4155.

[32] I. V. Anikin, "Information security risk assessment and management method in computer networks," in *2015 International Siberian Conference on Control and Communications (SIBCON)*, IEEE, May 2015, doi: 10.1109/sibcon.2015.7146975.

[33] D. E. I. Esparza, F. J. Diaz, T. K. S. Echeverria, S. R. A. Hidrobo, D. A. L. Villavicencio, and A. R. Ordonez, "Information security issues in educational institutions," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, Jun. 2020, doi: 10.23919/cisti49556.2020.9141014.

[34] W. Yang, S. Wang, X. Huang, and Y. Mu, "On the Security of an Efficient and Robust Certificateless Signature Scheme for IIoT Environments," *IEEE Access*, vol. 7, pp. 91074–91079, 2019, doi: 10.1109/access.2019.2927597.

[35] M. Yu *et al.*, "Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, Dec. 2018, doi: 10.1177/1550147718815842.

[36] M. A. Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, p. 155014771881505, Dec. 2018, doi: 10.1177/1550147718815054.

[37] P. P. do Nascimento, P. Pereira, J. M. Mialaret, I. Ferreira, and P. Maciel, "A methodology for selecting hardware performance counters for supporting non-intrusive diagnostic of flood DDoS attacks on web servers," *Computers & Security*, vol. 110, p. 102434, Nov. 2021, doi: 10.1016/j.cose.2021.102434.

[38] D. Ki-Aries, S. Faily, H. Dogan, and C. Williams, "Assessing system of systems information security risk with OASoSIS," *Computers & Security*, vol. 117, p. 102690, Jun. 2022, doi: 10.1016/j.cose.2022.102690.

[39] N. Cajkova, "A Soft Target Risk Application and Threat Analysis Methodology at the Faculty of Applied Informatics in Zlín," *Journal of Physics: Conference Series*, vol. 1603, no. 1, p. 12018, Sep. 2020, doi: 10.1088/1742-6596/1603/1/012018.

[40] Y. Guo *et al.*, "Research on Computer Network Risk Prevention and Control Technology in the Information Age," *IOP Conference Series: Earth and Environmental Science*, vol. 632, no. 4, p. 42057, Jan. 2021, doi: 10.1088/1755-1315/632/4/042057.

[41] P. Kuppusamy *et al.*, "Systematic Literature Review of Information Security Compliance Behaviour Theories," *Journal of Physics: Conference Series*, vol. 1551, no. 1, p. 12005, May 2020, doi: 10.1088/1742-6596/1551/1/012005.

[42] R. Wang, J. Fang, Z. Yang, and H. Li, "Multi Feature Selection based Network Traffic Anomaly Detection Method," *Journal of Physics: Conference Series*, vol. 1288, no. 1, p. 12003, Aug. 2019, doi: 10.1088/1742-6596/1288/1/012003.

[43] S. Borzenkova and A. Sychugov, "Methodology for determining a set of measures to ensure information security in the automated process control system," *Journal of Physics: Conference Series*, vol. 1679, no. 3, p. 32075, Nov. 2020, doi: 10.1088/1742-6596/1679/3/032075.

[44] A. McLeod and D. Dolezel, "Information security policy non-compliance: Can capitulation theory explain user behaviors?," *Computers & Security*, vol. 112, p. 102526, Jan. 2022, doi: 10.1016/j.cose.2021.102526.

[45] W. Mao and F.-Y. Wang, “Intelligence and Security Informatics,” in *Advances in Intelligence and Security Informatics*, Elsevier, 2012, pp. 1–7, doi: 10.1016/b978-0-12-397200-2.00001-4.

[46] A. Andersson, K. Hedström, and F. Karlsson, “Standardizing information security – a structurational analysis,” *Information & Management*, vol. 59, no. 3, p. 103623, Apr. 2022, doi: 10.1016/j.im.2022.103623.

[47] N. H. Hassan and Z. Ismail, “Information security culture in healthcare informatics: A preliminary investigation,” *Journal of Theoretical and Applied Information Technology*, vol. 88, no. 2, pp. 202–209, 2016.

[48] X. Sun, Z. Li, T. Chen, and Q. Huang, “Public security risk prevention and control support key technology research,” *IOP Conference Series: Earth and Environmental Science*, vol. 242, p. 52033, Mar. 2019, doi: 10.1088/1755-1315/242/5/052033.

[49] S. Kokolakis, D. Gritzalis, and S. Katsikas, “Generic security policies for healthcare information systems,” *Health Informatics Journal*, vol. 4, no. 3–4, pp. 184–195, Sep. 1998, doi: 10.1177/146045829800400309.

[50] J. Liu, H. Stewart, C. Wiens, J. Mcnitt-Gray, and B. Liu, “Development of an integrated biomechanics informatics system with knowledge discovery and decision support tools for research of injury prevention and performance enhancement,” *Computers in Biology and Medicine*, vol. 141, p. 105062, Feb. 2022, doi: 10.1016/j.compbiomed.2021.105062.

[51] R. L. M. J. S. Ali and J. Kaliappan, “Patient health informatics system using cloud computing and IoT,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 7, pp. 2162–2165, 2019.

[52] X. Xin, Y. Shu-Jiang, P. Nan, D. ChenXu, and L. Dan, “Review on A big data-based innovative knowledge teaching evaluation system in universities,” *Journal of Innovation & Knowledge*, vol. 7, no. 3, p. 100197, Jul. 2022, doi: 10.1016/J.JIK.2022.100197.

[53] N. A. H. Ghazali, S. S. M. Fauzi, R. A. JM. Gining, W. A. W. M. Sobri, and A. J. Suali, “Visualizing Software Risks in Software Engineering Projects using Risk Sensitivity Analysis Approach,” *Journal of Physics: Conference Series*, vol. 1529, no. 2, p. 22074, Apr. 2020, doi: 10.1088/1742-6596/1529/2/022074.

[54] R. Saxena and E. Gayathri, “A study on vulnerable risks in security of cloud computing and proposal of its remedies,” *Journal of Physics: Conference Series*, vol. 2040, no. 1, p. 12008, Oct. 2021, doi: 10.1088/1742-6596/2040/1/012008.

[55] J. Karro and Jie Wang, "Protecting Web servers from security holes in server-side includes," *Proceedings 14th Annual Computer Security Applications Conference (Cat. No.98EX217)*, Phoenix, AZ, USA, 1998, pp. 103-111, doi: 10.1109/CSAC.1998.738590.

[56] G. Lawton, “Stronger Domain Name System Thwarts Root-Server Attacks,” *Computer*, vol. 40, no. 5, pp. 14–17, May 2007, doi: 10.1109/mc.2007.184.

[57] S. S, S. Janakiraman, M. Srividya, and N. Anusha, “A contemporary network security technique using smokescreen SSL in huddle network server,” in *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, IEEE, Feb. 2016, doi: 10.1109/aeeicb.2016.7538376.

[58] N. K. Sehgal and M. Ganguli, “Applications of Virtualization for Server Management and Security,” in *2006 IEEE International Conference on Industrial Technology*, IEEE, 2006, doi: 10.1109/icit.2006.372614.

[59] M. Idhom, H. E. Wahanani, and A. Fauzi, “Network Security System on Multiple Servers Against Brute Force Attacks,” in *2020 6th Information Technology International Seminar (ITIS)*, IEEE, Oct. 2020, doi: 10.1109/itis50118.2020.9321108.

[60] R. M. Aslanov, “The right to information in the legislation of the Azerbaijan Republic,” *Computer Law & Security Review*, vol. 32, no. 6, pp. 888–897, Dec. 2016, doi: 10.1016/J.CLSR.2016.07.010.

[61] H. Kim, “Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks,” *International Journal of Distributed Sensor Networks*, vol. 8, no. 11, p. 268478, Jan. 2012, doi: 10.1155/2012/268478.

[62] R. Zhou, Y. Lai, Z. Liu, Y. Chen, X. Yao, and J. Gong, “A Security Authentication Protocol for Trusted Domains in an Autonomous Decentralized System,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 3, p. 5327949, Mar. 2016, doi: 10.1155/2016/5327949.

[63] N. P. Çiftçi and Ö. Delialioğlu, “Supporting students’ knowledge and skills in information technology security through a security portal,” *Information Development*, vol. 32, no. 5, pp. 1417–1427, Jul. 2016, doi: 10.1177/0266666915601463.

[64] Md. M. Hassan, B. R. Ahmad, A. Esha, R. Risha, and M. S. Hasan, “Important factors to remember when constructing a cross-site scripting prevention mechanism,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 2, pp. 965–973, Apr. 2022, doi: 10.11591/eei.v11i2.3557.

[65] S. Hisada *et al.*, “Surveillance of early stage COVID-19 clusters using search query logs and mobile device-based location information,” *Scientific Reports*, vol. 10, no. 1, Oct. 2020, doi: 10.1038/s41598-020-75771-6.

BIOGRAPHIES OF AUTHORS

Angel Namo-Ochoa Bachelor in Systems Engineering from Norbert Wiener University, Lima, Peru. He has several international publications. Specialized in the areas of augmented reality, virtual reality, internet of things, software development and computer science. Author of scientific articles indexed in IEEE Xplore and Scopus. He can be contacted at email: a2020102820@uwiener.edu.pe.

Eduardo Portilla-Cosar Bachelor in Systems Engineering at Norbert Wiener University, Lima, Peru. Specialized in the areas of computer science, software development, computer security, and mobile application development. He has several international publications. Author of several research papers. He can be contacted at email: a2020102844@uwiener.edu.pe.

Fernando Sierra-Liñan has a Bachelor's degree in Education, specializing in Science and Technology at USIL, a Master's degree in Edumatics and University Teaching at UTP, a Bachelor's degree in Systems Engineering and Computer Science at UTP, with a technical specialty in Computer Science and Computer Science. He is currently working as a researcher and thesis advisor in the faculty of Computer Engineering and Systems at the Universidad Privada del Norte, Lima - Peru. He has 20 years of teaching experience. His areas of interest are programming, database, and data analysis. He can be contacted at email: fernando.sierra@upn.edu.pe, pfsierra.D02052@gmail.com.

Michael Cabanillas-Carbonell Engineer and Master in Systems Engineering from the National University of Callao - Peru, Ph.D. candidate in Systems Engineering and Telecommunications at the Polytechnic University of Madrid. Ex-President of the chapter of the Education Society IEEE-Peru. Conference Chair of the Engineering International Research Conference IEEE Peru EIRCON. Advisor and Jury of Engineering Thesis in different universities in Peru. International lecturer in Spain, United Kingdom, South Africa, Romania, Argentina, Chile, China. Specialization in software development, artificial intelligence, machine learning, business intelligence, augmented reality. Reviewer IEEE Peru and author of more than 100 scientific articles indexed in IEEE Xplore and Scopus. He can be contacted at email: mcabanillas@ieee.org.