BOHR International Journal of Smart Computing and Information Technology
2021, Vol. 2, No. 1, pp. 39–45
DOI: 10.54646/bijscit.2021.17
www.bohrpub.com

METHODS

An improved intelligence approach to handling data leakage risks in the corporate information security process

T. Kiruthiga[1]*, A. Vaniprabha[2] and M. Sutharsan[3]

[1]Department of Electronics and Communication Engineering, Vetri Vinayaga College of Engineering & Technology, Tholurpatti, India
[2]Department of Electronics and Communication Engineering, SNS College of Engineering, Coimbatore, India
[3]Department of Electronics and Communication Engineering, Muthayammal Engineering College, Rasipuram, India

***Correspondence:**
T. Kiruthiga,
drkiruthigaece@gmail.com

Received: 25 June 2021; **Accepted:** 10 July 2021; **Published:** 22 July 2021

Confidential information is of great interest to competing firms. This causes aggression and attacks. Many people underestimate the importance of the threat, and as a result, it can lead to collapse and bankruptcy for the company. Even a single case of malpractice can result in millions in damages and the loss of customer trust. Threats are subject to data on organization structure, status, and operations. Sources of such threats are its competitors, corrupt officials, and criminals. They are introduced with certain value-protected information and modified in order to cause financial damage. Even 20% of such a decision can result in information leakage. Sometimes the loss of company secrets can be due to the inexperience of employees or a lack of security systems. In this paper, an improved intelligence approach to handling data leakage risks in the corporate information security process is proposed. Accounting automatically calculates weighted relative class systems through a complete, complex security of the most important processes and technical and organizational measures. Their combination is an antivirus system, a firewall, and protection from electromagnetic radiation. Systems protect information on electronic media sent through communication channels, access exemptions for various documents, create backup copies, and recover confidential information after damage.

Keywords: information, security, aggression, attack, threat, financial damage, data, leakage, risk.

Introduction

Security are developed for security and to prevent data loss in the field of information security (1). Their work is based on complex software systems that prevent any data loss. The exclusivity of the program requires the elimination and debugging of the internal circulation of data and documents (2, 3). Security analysis of all steps when using information is based on working with databases.

Information security can be ensured with the help of online funds, as well as products and solutions offered on all types of Internet resources (4). The developers of some services have been able to effectively package an information security system that protects against external and internal threats, while ensuring the right balance of price and functionality (5, 6). The proposed flexible modular complexes combine the functionality of hardware and software.

The organization's information security should be fully controlled year round, in real time, around the clock (7). At the same time, the system takes into account the entire life cycle, starting from the moment of appearance and ending with complete destruction and loss of significance for the company (8).

For the top management and owners of the companies, there was only one problem to comply with (and the only way to accomplish it was to perform the low-cost proposed requirements) (9). For recognized bodies, a problem arose: the impossibility of all possible actions and conditions of

their implementation, as well as significant differences in the scope of actions, made it impossible to propose a universal set (10, 11).

For this, the information security problem was considered a self-sufficient entity, with activities, objectives, conditions, and practices substantially contributing to the satisfaction of universal needs (12). Both approaches (institutions and regulators) are inadequate and represent a significantly distorted reality (13). Thus, the main substantive restrictions on information security systems are related to the traditional IP model, which implies the mandatory presence of an attacker focused on protecting the information of damaged assets (information) and, accordingly, the actions of such a subject (in the subjects of subjects) (14–16).

In this case, for example, application-related incidents cannot be attributed to attacks with routine changes in application software (17). Their possible reasons are weakly developed management and a weak technical base. The system of current conditions (management, processes of the main operation) is usually the most powerful source of problems, which are ignored due to the non-binding nature of the attack (18–20).

Further evolution of information security system models strengthened the tasks of the owner, who chose himself, that is, from a standard set of such security measures that in his opinion, could provide an acceptable level of security (21–23). This was a significant step because it provided an information security system bond to a specific object with specific conditions for its existence as well as the contradictions associated with the information security system problem's self-sufficiency (24, 25).

However, no configuration mechanism is provided for the owner, except to create a list of objects with selected common security measures (security profiles) (26). Professionals developed an expert-curing system. At the same time, how the risk affected the owner, was both unknown and practically determined (27, 28).

Literature review

All entrepreneurs always seek to provide information and confidentiality. To develop appropriate information security, the nature of potential threats is taken into account, as well as the methods of their occurrence (29). The information security system of the company is done in such a way that a group can meet the hacker protection levels. As a result, an attacker cannot penetrate the protected area (30).

A more efficient way to protect information is to include a crypto-resistant encryption algorithm during data transmission. Computer data encrypts itself and cannot be accessed; it is private (31). The structure of access to information should be multi-leveled, according to which selected employees are allowed access (32). Only those with complete access to all information should have a decent face.

The list of information related to confidential information is approved by the head of the company (33). Any violations in this area will have to overcome certain obstacles. It should be kept in mind that cheap wireless networks cannot provide the required level of security (34).

Appropriate and frequently integrated actions provide security models. Currently, special applications are being developed around the round-the-clock monitoring status of the network and the warning of information security systems (35). Managers should conduct training exercises to avoid accidental data collection by employees.

It plans employee readiness and allows managers to have confidence that all employees can comply with information security measures (36). The atmosphere of the market economy and a high level of competition make company executives always alert and quick to respond to any difficulties. In the last 20 years, information technologies have been able to enter all areas of development, management, and business management (37).

In the real world, the business has long since become a virtual one, but it should be remembered how popular it is in its own right (38). Currently, virtual threats to an organization's information security can cause it incredibly real harm. Underestimating the problem, leaders risk their businesses, reputations, and power (39).

Most companies usually suffer damage due to data leakage. The security of an organization's information should take priority over the course of a business and its maintenance. Information security is critical to success, profitability, and achieving company goals (40).

Proposed model

Pragmatic information security system models are known to be based on an assessment of the owners' total costs and an assessment of the "return" on investments in the information security system. Within the framework of this approach, a group of organizations that are close to the objectives and conditions of the organizations cite the means of implementing information security systems, and create a model that includes best practices in the group. Also, it determines the direction and level of investment based on best practices, their conditions (occurring events), and their aftermath.

Problem formation

Sometimes the employees of the companies can provoke special internal leaks showing their dissatisfaction with their salary, work, or colleagues. It can easily provide all the valuable information to its competitors, try to destroy it, or deliberately create a virus on the computers. Information that

is the property of the company may be threatened. The data leakage problem was shown in **Figure 1**.

Threats to confidentiality of information and plans

Illegal access to data, communication channels, or programs can happen later. Data from or transmitted from a computer can be intercepted through leaky channels. It uses special equipment that creates an analysis of electromagnetic emissions received while working on a computer.

Risk of damage

Illegal activities by hackers may result in compensation or the loss of transaction or transmission information.

Threat access

Such situations do not allow the legitimate user to use the services and resources. This occurs after they have been captured, whether to obtain data or to block lines by intrusions. Such an incident could distort the accuracy and timeliness of the information being disseminated.

Risk of refusal to execute transactions

The user opts out of receiving the same information in order to avoid liability.

Domestic threats

Such threats pose a high risk to the organization. They are perpetuated by inexperienced leaders, incompetent, or incompetent employees.

Proposed approach

The information security system model proposed in the standard advances this issue in terms of expanding the definition of "attack" as part of its integration. Under the attack, it is understood as a person who has a conflict with the owner and has his/her own goals, and who will gain control over the assets of the organization.

This approach significantly expands the types and sources of damages that can enter the area under consideration for the information security system, and their resolution is more rational. The logic of operation of information security systems includes the following actions (**Figure 2**):

- Prediction and rapid recognition of threats to the security of data, intentions, and conditions that have caused damage to the organization and concrete failures in its work and development
- Creating such working conditions in which the level of risk and the possibility of damage to the organization are minimized
- Compensation for damage and minimizing the impact of identified damage initiatives

However, he/she often requires a compromise approach, and the final result of the final product is a more approximate IP issue. Through the creation and maintenance of a secure and reliable information sphere, including the struggle with an attack, it directly contributes to its effectiveness and helps in the necessary improvement. Only one such model can be realized by the business. No one else repeats them. Information security tools can include the following, as shown in **Figure 3**.

- Technical
- Software
- Cryptography
- Institutional
- Assembly

Any form of business is always fraught with risk. At the same time, a good leader does not wait for problems—it

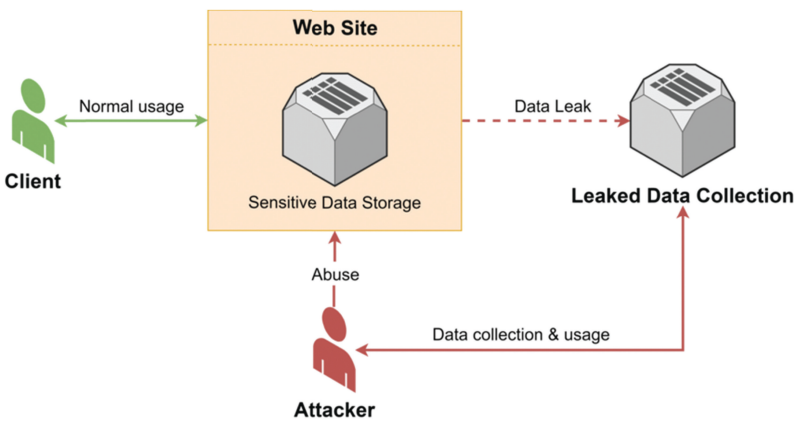

FIGURE 1 | Data leakage problem.

often takes timely measures to protect against problems in the business sector. This is because:

- Corporate problems: conflicts and conflict situations between the shareholders of the company, conflicts between top managers, the complexity of the relationship between the owners of the company, and the complexity of the relationship between the heads of division;
- External dangers: threats from criminal structures, conflicts with law enforcement and state structures, raiders, and so on;
- Financial losses: fraudulent actions of employees (customers), theft, unfair intermediaries or suppliers, inappropriate use of company resources, taking bribes for certain actions against the interests of the company;
- Information risks: leakage (its concealment or destruction) of confidential company information, unauthorized access to confidential data, disclosure of trade secrets, and the like;
- Security "players": theft of material and technical assessments by unauthorized persons, unauthorized intrusion into the territory of the enterprise, and violation of labor discipline; and
- Reputational problems: In the framework of workers with a bad reputation, the cooperation of workers with a bad reputation has a bad reputation.

Further evolution reduced it to the laboratory that the information security system could create damage for the purpose of action, so the risks of the information security system (which were self-sufficient) had to agree with the company's risks. It is only intended to indicate how the information security system should be integrated into enterprise-wide corporate management, not as an isolated and independent process but as an integrated and strongly related component of management.

This cannot be done. However, this approach has improved several categories of IB, including the risks of information security systems. To solve the listed business problems, the following types of security are required:

- Physical—security systems, security, surveillance cameras, and so on;
- Economic—counterparty verification, customer bank security, and tax optimization;
- Organizational and personnel—verification of employees entering employment and control of existing employees;
- Information—intrusion protection, files and documents protection, optimization and security 1C, single authentication, protection against information leakage, and more; and
- Legal—checks the validity of transactions, documents, plans of subscription service, and more. Investors' performance is assessed to minimize damage from events in the investment sector in the next period and therefore limit large losses. However, their advantages are that a diverse approach is required for a wide exchange of important information and that participants with conflicts of interest avoid creating any quality trust measures, so they are not widespread.

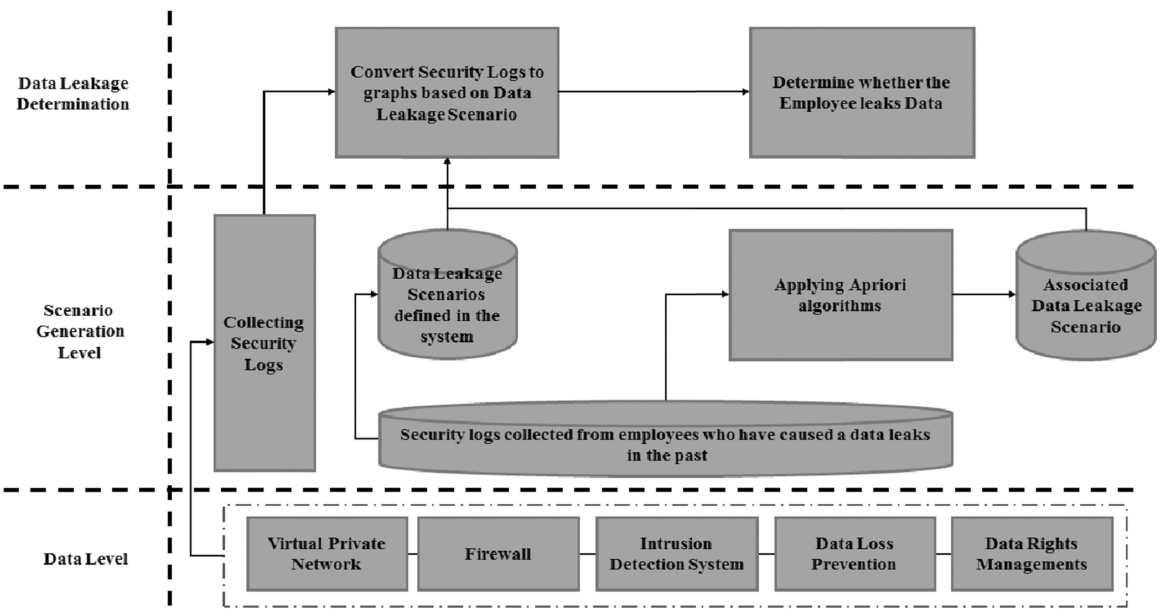

FIGURE 2 | Proposed improved intelligence approach.

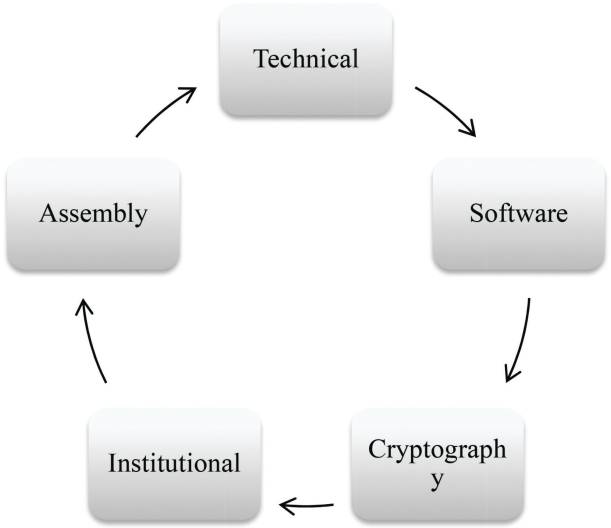

FIGURE 3 | Information security tools.

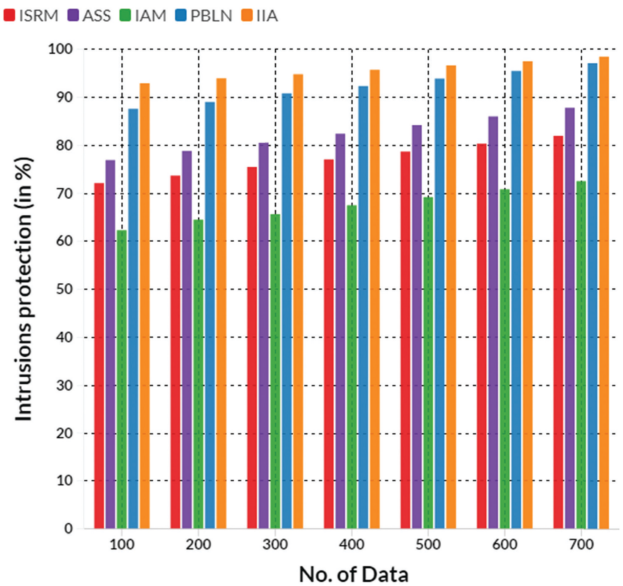

FIGURE 4 | Comparison of intrusion protection.

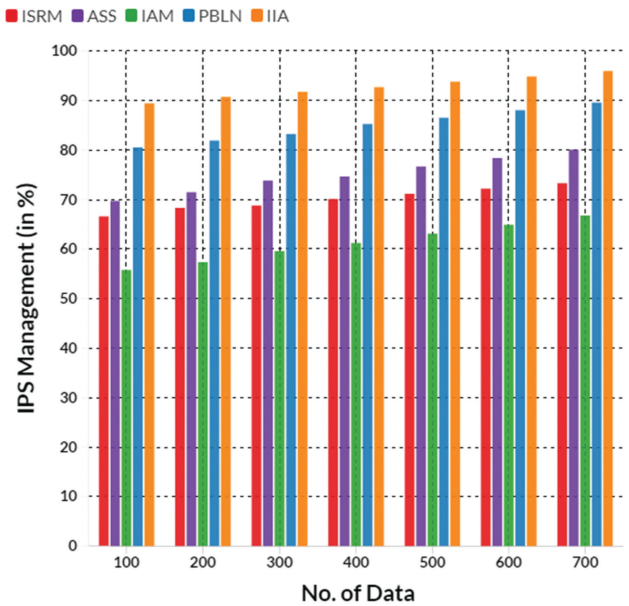

FIGURE 5 | Comparison of IPS management.

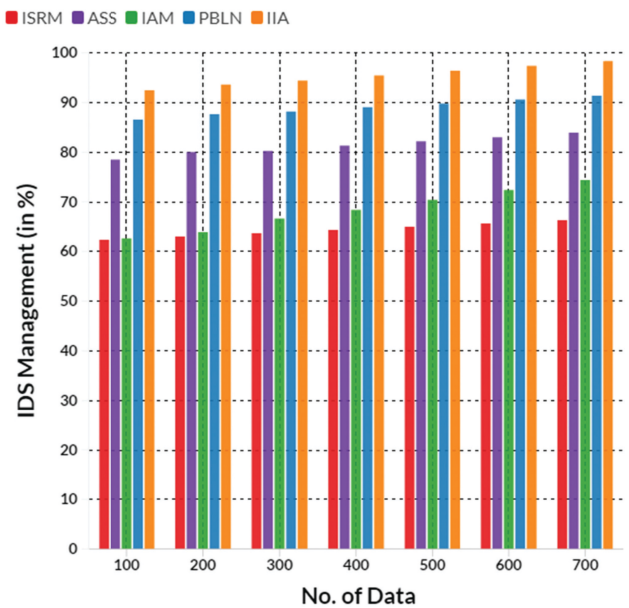

FIGURE 6 | Comparison of IDS management.

Results and discussion

According to statistics, more than half of all business problems are caused by "gaps" in information security. Leakage of information to competitors, loss of data, and transfer of confidential company information into the hands of other people—all this is a big risk for business.

In such a situation, IT management companies take many effective measures to ensure the comprehensive security of the company. The proposed improved intelligence approach (IIA) was compared with the existing information security risk management (ISRM), antivirus security systems (ASS), identity access management (IAM), and protocol-based local networks (PBLN).

Intrusion protection

Installing necessary programs or equipment to control traffic on the network. When the first danger appears (an invasion), the system responds and blocks access. At the same time, the responsible employee is notified. This is depicted in Figure 4 below.

IPS Management

Its task is to block any network activity that causes suspicion of "extra" traffic. Plus, systems have not only the ability

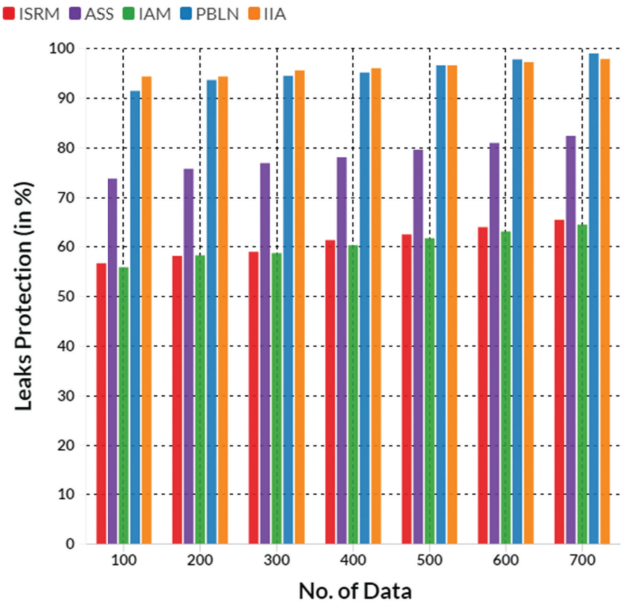

FIGURE 7 | Comparison of leaks protection.

to detect but also the ability to prevent invasion. Minus systems have a high percentage of incorrect positioning, which leads to the continuous elimination of idle employees from business at the time of computer network verification. This is shown in the following **Figure 5**.

IDS Management

Monitoring of ongoing conflicting activity when alerted to the administrator. Positive aspects are the effective fight against invasion and the transfer of rights to the decision of the administrator. Deductions mean that responsible workers do not have time to take action, and the system can cause undue harm. **Figure 6** shows an example of this.

Leaks protection

A set of safeguards designed to prevent unauthorized access to confidential information. Due to the lack of personnel (the loss of the carrier, sending a password by mail, switching to a page with a virus, etc.), **Figure 7** shows an example of this.

Furthermore, to protect against random errors, it is critical to organize, register—it is critical to register PCS, encryption USB cards, RMS application, DLP system introduction, and more.

Conclusion

The information resources of most organizations are among the most valuable sources. For this reason, commercial, confidential information, and personal data must be reliably protected from illegal use but at the same time easily accessible by using it to perform the tasks involved in the processing of this information or assigned to it. Use of these specialized methods contributes to the sustainability of the company's business and its credibility.

As practice shows, the issue of organizing commercial security is very relevant in modern conditions. Online shopping and dedicated shoppers' credit cards, casinos, and duds are under threat; corporate networks are falling under external management; computers are attacked and included in bot networks; and fraud using hijacked personal data is a national disaster.

Therefore, managers of organizations should be aware of the importance of information security, and forecasting trends in this area and managing them are considered important processes.

References

1. Grishaeva SA, Borzov VI. Information security risk management. *Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*. Yaroslavl: IEEE (2020). p. 96–8.
2. Ramesh G, Logeshwaran J, Aravindarajan V. The performance evolution of antivirus security systems in ultra dense cloud server using intelligent deep learning. *BOHR Int J Comput Intell Commun Netw.* (2022) 1:15–9.
3. Mohammed IA. Systematic review of identity access management in information security. *Int J Innovat Eng Res Technol.* (2017) 4:1–7.
4. Ramesh G, Logeshwaran J, Gowri J, Mathew A. The management and reduction of digital noise in video image processing by using transmission based noise elimination scheme. *ICTACT J Image Video Process.* (2022) 13:2797–801.
5. Nechai A, Pavlova E, Batova T, Petrov V. Implementation of information security system in service and trade. *Proceedings of the IOP Conference Series: Materials Science and Engineering.* (Vol. 940), Bristol: IOP Publishing (2020). 012048 p.
6. Logeshwaran J. The topology configuration of protocol-based local networks in high speed communication networks. *Multidiscip Approach Res.* (2022) 15:78–83.
7. Noghondar ER, Marfurt K, Haemmerli B. The human aspect in data leakage prevention in academia. *ISSE 2012 Securing Electronic Business Processes.* Wiesbaden: Springer Vieweg (2012). p. 137–46.
8. Prem Anandh A, Ramesh G, Logeshwaran J, Kiruthiga T. Impact of multiple disciplinary researches in Maritime Sector. *Multidiscip Approach Res.* (2022) 13:74–80.
9. Yildirim E. The importance of information security awareness for the success of business enterprises. *Advances in Human Factors in Cybersecurity*. Cham: Springer (2016). p. 211–22.
10. Ramesh G, Logeshwaran J, Rajkumar K. The smart construction for image pre-processing of mobile robotic systems using neuro fuzzy logical system approach. *NeuroQuantology* (2022) 20:6354–67.
11. Alneyadi S, Sithirasenan E, Muthukkumarasamy V. A survey on data leakage prevention systems. *J Netw Comput Applicat.* (2016) 62:137–52.
12. Raja S, Logeshwaran J, Venkatasubramanian S, Jayalakshmi M, Rajeswari N, Olaiya NG, et al. OCHSA: designing energy-efficient lifetime-aware leisure degree adaptive routing protocol with optimal cluster head selection for 5G communication network disaster management. *Sci Program.* (2022) 2022.

13. Johnson ME, Goetz E, Pfleeger SL. Security through Information Risk Management. *IEEE Secur. Priv.* (2009) 7:45–52.
14. Gopi B, Logeshwaran J, Gowri J, Kiruthiga T. The moment probability and impacts monitoring for electron cloud behavior of electronic computers by using quantum deep learning model. *NeuroQuantology.* (2022) 20:6088–100.
15. Trang MN. Compulsory corporate cyber-liability insurance: outsourcing data privacy regulation to prevent and mitigate data breaches. *Minn JL Sci Tech.* (2017) 18:389.
16. Gopi B, Logeshwaran J, Gowri J, Aravindarajan V. The Identification of quantum effects in electronic devices based on charge transfer magnetic field model. *NeuroQuantology.* (2022) 20:5999–6010.
17. Morse EA, Raval V, Wingender JR Jr. Market price effects of data security breaches. *Informat Secur J A Global Perspect.* (2011) 20:263–73.
18. Logeshwaran J, Malik JA, Adhikari N, Joshi SS, Bishnoi P. IoT-TPMS: an innovation development of triangular patient monitoring system using medical internet of things. *Int J Health Sci.* (2022) 6:9070–84.
19. Elachgar H, Regragui B. Information security, new approach. *Proceedings of the Second International Conference on the Innovative Computing Technology (INTECH 2012)*. Casablanca: IEEE (2012). p. 51–6.
20. Ramesh G, Aravindarajan V, Logeshwaran J, Kiruthiga T, Vignesh S. Estimation analysis of paralysis effects for human nervous system by using Neuro fuzzy logic controller. *NeuroQuantology.* (2022) 20:3195–206.
21. Kulkarni G, Gambhir J, Patil T, Dongare A. A security aspects in cloud computing. *Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering*. Casablanca: IEEE (2012). p. 547–50.
22. Sekar G, Sivakumar C, Logeshwaran J. NMLA: the smart detection of motor neuron disease and analyze the health impacts with neuro machine learning model. *NeuroQuantology.* (2022) 20:892–9.
23. Park S. Why information security law has been ineffective in addressing security vulnerabilities: evidence from California data breach notifications and relevant court and government records. *Int Rev Law Econ.* (2019) 58:132–45.
24. Jasmine J, Yuvaraj N, Logeshwaran J. DSQLR- A distributed scheduling and QoS localized routing scheme for wireless sensor network. *Recent Trends in Information Technology and Communication for Industry 4.0*. (Vol. 1), Chennai: RcHuB Publications (2022). p. 47–60.
25. Hashimoto GT, Rosa PF, Lopes Filho E, Machado JT. A security framework to protect against social networks services threats. *Proceedings of the 2010 Fifth International Conference on Systems and Networks Communications*. Nice: IEEE (2010). p. 189–94.
26. Ramkumar M, Logeshwaran J, Husna T. CEA: certification based encryption algorithm for enhanced data protection in social networks. *Fundament Appl Mathemat Soft Comput.* (2022) 1:161–70.
27. Bhaharin SH, Asma'Mokhtar U, Sulaiman R, Yusof MM. Issues and trends in information security policy compliance. *Proceedings of the 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. Johor Bahru: IEEE (2019). p. 1–6.
28. Logeshwaran J. The control and communication management for ultra dense cloud system using fast Fourier algorithm. *ICTACT J Data Sci Mach Learn.* (2022) 3:281–4.
29. Fazlida MR, Said J. Information security: risk, governance and implementation setback. *Proc Econ Finance.* (2015) 28:243–8.
30. Sutharasan M, Logeshwaran J. Design intelligence data gathering and incident response model for data security using honey pot system. *Int J Res Dev Technol.* (2016) 5:310–4.
31. Stamati-Koromina V, Ilioudis C, Overill R, Georgiadis CK, Stamatis D. Insider threats in corporate environments: a case study for data leakage prevention. *Proceedings of the Fifth Balkan Conference in Informatics*. New York, NY: Association for Computing Machinery (2012). p. 271–4.
32. Logeshwaran J, Saravanakumar K, Dineshkumar S, Arun-prasath C. SBML algorithm for intelligent fuel filling (IFF) and smart vehicle identification system (SVIS). *Int J Adv Res Manage Arch Technol Eng.* (2016) 2:149–54.
33. Neghina DE, Scarlat E. Managing information technology security in the context of cyber crime trends. *Int J Comput Commun Control.* (2012) 8:97–104.
34. Logeshwaran J, Rex MJ, Kiruthiga T, Rajan VA. FPSMM: fuzzy probabilistic based semi morkov model among the sensor nodes for realtime applications. *Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS)*. Palladam: IEEE (2017). p. 442–6.
35. Ibnugraha PD, Nugroho LE, Santosa PI. Risk model development for information security in organization environment based on business perspectives. *Int J Informat Secur.* (2021) 20:113–26.
36. Logeshwaran J, Shanmugasundaram RN. Enhancements of resource management for device to device (D2D) communication: a review. *Proceedings of the 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. Palladam: IEEE (2019). p. 51–5.
37. Kauspadiene L, Ramanauskaite S, Cenys A, Janulevicius J, Rastenis J. Modeling of enterprise management structure for data leakage evaluation. *Informat Secur J.* (2018) 27:1–13.
38. Logeshwaran J. AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. *ICTACT J Data Sci Mach Learn.* (2021) 3:251–3.
39. Singh AN, Picot A, Kranz J, Gupta MP, Ojha A. Information security management (ism) practices: lessons from select cases from India and Germany. *Glob J Flexible Syst Manage.* (2013) 14:225–39.
40. Logeshwaran J, Ramkumar M, Kiruthiga T, Sharanpravin R. The role of integrated structured cabling system (ISCS) for reliable bandwidth optimization in high-speed communication network. *ICTACT J Commun Technol.* (2022) 13:2635–9.