Journal of Applied Research and Technology

www.jart.icat.unam.mx

ICAT Instituto de Ciencias Aplicadas y Tecnología

Journal of Applied Research and Technology 20 (2022) 570-575

Original

Cognitive intelligence for interrogation and inflation of information security: A survey

Jayaganesh Jagannathan* • M. Y. Mohamed Parvees

Department of Computer and Information Science,
Annamalai University, Tamilnadu, India

Received 11 21 2020; accepted 06 24 2022
Available 10 31 2022

Abstract: Information security is the set of forms that secure data faraway from illegal connection, revelation, duplication, alteration. As of late, increasingly legitimate frameworks such as resourceful inter and intra urban city, remote sensor systems, authentication digital signature frameworks, and superintendence, have recently needed data security affirmations. Hence, over the past research, numerous diverse strategies focused on cognitive intelligence are created for data security. In any case, there are not complete reviews which recapitulate strategies. In this way, this document surveyed on cognitive intelligence move toward presented on publications and symposiums for data security within most recent years. This article gives a precise review to audit various cognitive intelligence access and applications of data security. In additionally, deliberate the threat of cognitive intelligence access and applications for data security is conferred.

Keywords: ANN, cognitive intelligence, data security, genetic programming, information security

*Corresponding author.
E-mail address: everjays@gmail.com(Jayaganesh Jagannathan).
Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

Information security is the set of forms that secure data faraway from illegal connection, revelation, duplication, alteration. It is intended to preserve in different ways, Confidentiality (c), Integrity (I), and Availability (A) of trade information (Andress, 2014; Junaid et al., 2022). As such, data security systems are developed around the center destinations of CIA triad is guaranteeing private data is just revealed to approved people (C), forestalling unapproved alterations to private data (I), and ensuring that data is accessed when requested by approved individuals (A) (Ahmad et al., 2014; Thaler et al., 2018).

As of late, increasingly legitimate frameworks such as resourceful inter and intra urban city, remote sensor systems, authentication digital signature frameworks, and superintendence, have recently needed data security affirmations (Cao et al., 2012; Tao et al., 2018). Be that as it may, the expanding measures of data and the expanding sophistication of data have become significant difficulties in data security. So as to conquer these difficulties numerous cognitive intelligence strategies just as other AI methods are planned. Artificial Intelligence involves a collection of commonly used techniques for data investigation that computerize the creation of systematic models. Artificial Intelligence approaches are: study the data, distinguish designs, and build choices with stripped-down human being mediation.

Cognitive intelligence is an associate domain of artificial intelligence, is look at of intellectual system that may demonstrate smart practices in composite and shifting situation. In particular cognitive intelligence frames a group of environment motivated computing strategies ways to deal with illuminating complex certifiable information driven issues which can be tough to remedy physically through conventional representation (Iqbal et al., 2018).

Cognitive intelligence unites 2 interior methods to generate intellectual systems: artificial neural networks (ANN) and emotional computation intelligence. Expansion in this direction of these 3 primary methods; Modern reckoning intelligences includes methods, for example, the half and halves of the above mentioned. These methods to cognitive intelligence are effectively utilized to resolve several issues in data security, for example looking an ideal arrangement, categorizing ordinariness and variation from the norm in an interruption location framework and information stowing away (El-Alfy & Awad, 2016).

2. Background

Data security purpose is to ensure data deficient from unconstitutional access, confession, duplication, alteration or pulverization, and preserve the CIA set of three of business information in its different forms (Andress, 2014; Thaler et al., 2018). Numerous data security methods are recently described and categorized in a number of modes, and the description or categorization is not entirely decided on. A. Ahmad, S. B. Maynard, and S. Park (Ahmad et al., 2014) recapitulated a sequence of data security methods together with deterrence, supervision, recognition, reaction, and extortion. In multiple cases, these techniques may be used to hold networks protected with potential security concerns throughout important to maintain that customers have consistent service access. Table I summarizes the concepts and the reference of these methods for data security. Cognitive intelligence can also be used for these techniques to be applied. The following subsections provide a brief overview of these approaches.

Table 1. Description and survey of data security approaches.

Approaches	Description and survey
Deterrence	The purpose of deterrence is to insulate data from unconstitutional access, confession, duplication, alteration or pulverization (Siddique & Adeli, 2013; Suthir & Janakiraman, 2018)
Supervision	The structured observation of data is utilized by supervision, have been modeled to distinguish improvements to adjust to quick changing situations and hazards (Kumar, 2018; Suthir et al., 2016)
Recognition	Recognition is an organizational stage method order to assess particular security acts (Cavusoglu et al., 2005)
Reaction	Reaction points to require fitting remedial operations for distinguish tasks (D'Arcy et al., 2014)
Extortion	Extortion exploit baits to divert aggressors consideration from basic data to taken a toll the aggressors time and possessions (Siddique & Adeli, 2013; Tao et al., 2018)

3. Cognitive Intelligence for Information security

Cognitive intelligence is look at of intellectual system that may demonstrate smart practices in composite and shifting situation (Iqbal et al., 2018; Kulkarni et al., 2010). The ability to grasp and analyze information and utilize it consciously is cognitive intelligence. Although cognitive technology originated years back, a number of initiatives to cognitive computing were being created. The crucial strengths that your brain uses to understand, interpret, absorb, recall, think, and actually listen are cognitive abilities. Acting closely, together helps to establish data and share it to a source of knowledge which you use all day at academics, at profession, and then in daily existence. A few highlights that intellectual frameworks may communicate are:

Versatile: study as data changes, objectives and prerequisites progress. They may resolve vagueness and endure irregularity. They might be designed to benefit from dynamic data in real time, or close to real time. *Interactive:* They can communicate effectively with consumers so that they can confidently identify their desires. They can also communicate with other computers, networks, and cloud resources, as well as humans. *Iterative and stateful:* They can help to identify a situation and ask queries or merely seeking reference feedback is if research problem is unclear or inadequate. They will "recognize" past experiences in a mechanism and retrieve data that is pertinent for a specific project at a certain moment in time. *Contextual:* They can recognize and retrieve discrete features such as purpose, syntax, time, place, domain, rules, user information, method, role and target. They can rely on numerous information sources, both at structured and unstructured electronic data, and even some sensor inputs (visual, gestural, auditory or sensor provided).

Perhaps a stronger brand towards narrow minded Artificial Intelligence to be used exclusively for these narrow-minded applications is cognitive technology. Instead of attempting to develop AI, businesses are using cognitive technologies to automate and activate a broad array of challenge domains which require various sort of cognition. In certain terms, artificial intelligence seems to be about offering technological solutions for the challenges that seem to be intellectual, while cognitive intelligence mimics real intelligence to some extent through the use of such cognitive methods, such as Artificial Neural Networks (ANN) and Emotional Computation Intelligence (ECI) (Iqbal et al., 2018; Kulkarni et al., 2010).

3.1. ANN for data security

The artificial neural network plays a prominent significant task in the management of the network. It all Study in the field of intrusion detection systems largely depends on Artificial Intelligence systems for architecture, development, implementation and strengthen the security surveillance scheme. An artificial neural network includes a number of repetitions that transition a number of inputs into a set of appropriate permutations, transmits across a series of basic processors, or modules and relations among each other. Categories of the functions Iteration is inputs nodes, output, and modules among input and output form hidden units; correlation between the 2 modules given some size, had to decide how often one module impacts the other.

ANN comprises of an assortment of preparing units (neurons) (Wu & Banzhaf, 2010). In ANN, these preparing units/ neurons are to model a human brain neural network such that a robot can remember stuff and make human decisions (Yakura et al., 2018; Yang & Eickhoff, 2018). Although these neurons can be strongly interlinked in a given topology, ANN has been effectively applied to a wide scope of data demanding appliances (Choudhary & Swarup, 2009).

3.2. Emotional computation intelligence

Emotional computation intelligence is the capacity to interact, regulate our individual impulses, and communicate to others in a manner that demonstrates the role outlooks play in how individuals decide. The value of emotional computation intelligence is commonly regarded in several domains, like curriculum, business development and vending. Yet it's sort of rare to study about emotional intelligence in cyber security. But its participate in an essential part for the reason that humans are still at the core of efforts to maintain data secure, and hackers take part in on client concern to achieve admittance to top secret information. Here are only a couple instances of how emotional intelligence becomes an integral factor in information security.

According to Verizon's 2019 Internet Security Threat Report, phishing is the leading threat vector, despite people who have fallen for malware intended to defeat cyber protection steps. Attackers are becoming more socially intelligent; professional cyber attackers are observing why potential suspects indulge in targeted hacks and establish further effective manipulations. First ever task is to recognize the importance emotional computation intelligence performs in information security and to search at opportunities to implement emerging trends. Here are few ideas on using emotional computation intelligence to improve information security and counter attacks. All those experts predict Artificial Intelligence to solve the vulnerabilities that other information protection techniques have not completely overcome. But as long as the human factor exists, emotional computation intelligence can be a vital aspect of a successful information security policy.

4. Cognitive intelligence appliances in information security

As of late, an ever increasing number of frameworks in reality require the affirmations of information security, for example, Smart IoT and Health Care frameworks (Cao et al., 2012; Tao et al., 2018). Dissimilar to the appliances referenced over, these frameworks require a blend of different cognitive intelligence ways to deal with guarantee information security. In this part, survey a few frameworks, wherein cognitive intelligence approaches are utilized to ensure the appliances framework security.

4.1. Smart IoT

As of late, an ever increasing number of frameworks in reality require the affirmations of information security, for example, Smart IoT and Health Care frameworks. Dissimilar to the appliances referenced over, these frameworks require a blend of different cognitive intelligence ways to deal with guarantee information security. In this part, survey a few frameworks, wherein cognitive intelligence approaches are utilized to ensure the appliances framework security. Cognitive Artificial Intelligence agents may provide depth perception to machines and help them focus on solving issues (Sonawane et al., 2012). A further illustration is a sea oil refinery with massive amounts of data that would need to be attached to provide information. The machine may not have strong internet connectivity, so the AI cloud provider will be out. Information has to be on advanced machines so that they might detect unsafe conditions and intervene to avoid hazards in real time.

4.2. Health care

The core business perception of the challenges and benefits posed by developments in cognitive intelligence, AI and machine learning is not healthcare (Yang & Eickhoff, 2018). Cognitive engineering seems to be the latest development in the area of healthcare. It is a peer application that uses data mining techniques, pattern recognition, processing of natural language and human senses, and refining of the device depending on the real-time security of patient reports provide information. Cognitive intelligence is transforming the delivery of healthcare worldwide, and these systems use computational models to improve cognitive perspectives (Yang & Eickhoff, 2018).

Cognitive phenomenon is currently being used in leading innovators oncology centers across the world, the use of data sources (information that is heavy and not organized in a definite manner for even the most part, with even more than 80 percent of health information being defined as such), data on professional standards, reported clinical research, and data on clinical trials enable. In their statement, it seems to be a clinical governance aid system for clinicians. A number of advantages that endorse a Clinical Trials concept are offered by cognitive technologies in healthcare:

-Improves doctor-patient interaction, particularly through online platform,

-Manages data effectively by collecting significant medical expertise from multiple sources (clinical trial studies, medical blogs, etc.)

- Integrates detailed records with unstructured patient information, medications, medicines, etc.

- Provides access to important data regarding emerging trends, medical threats and health advancements

-Last but it's not most, it blends science data with personalized medical information to determine it available and usable for medical consultation.

The cognitive computing categorizes as 5 factors:

Offer type: Hardware, software, services.

Expertise: Natural language processing, deep learning, processing of context-aware, and system querying

Appliances: It may include preliminary diagnosis, robot-assisted surgery, virtual nursing assistant, recognition of patient clinical trials, dosage error reduction, Administrative workflow assistance, Fraud detection, etc.

User: Healthcare provider, Agency for pharmaceutical and biotechnology, Payer, where each has a particular purpose.

Type of the Product: Machine learning, Data extraction, Analysis, Recognition of optical characters, Processing and training of languages, Speech recognition, Computer vision, automated planning

Topography: Wise Division Region or Areas.

However, like any technical product, this too, has some significant barriers to overcome. These issues need to be tackled for smooth future adoption, in addition to man's fear of adapting to changing thoughts and getting anxious thoughts. *In the principal problems are:*

Protection: In the age of technology, protection will always be an issue and thus a top consideration. In order to manage a large amount of information, proper encryption process and protection must be available.

Agreement: For this a number of partnerships must be made between the people and government for reliable performance.

Up-gradation: Because of the noticeable, natural instinct, man is afraid that one day could destroy him, as his main goal is to imitate the rational thought cycle. Although what he fails to realize is that cognitive phenomenon is built to work and have a symbiosis in harmony with humans.

Extended Improvement Sequence: As a generic approach, cognitive computing is increasingly being explored and investigated. For a broader spectrum of sectors, this would not have the obvious benefit or versatility of handling scenario-based situations. Development cycles are gradually becoming shorter over time (Choudhary & Swarup, 2009; Yang & Eickhoff, 2018).

The Third Computing Era is known as Cognitive Technology. It would eliminate the time and travel constraints of doctors and patients by getting robots trained with organizational abilities, allocating frequent clinical trial evaluations, and drug discoveries that resolve complex health care procedures. In reducing the cost of delayed diagnosis and sub-optimal care choices, it also has value benefits. Soon, this transformation will be considered preferable, common practice, decision-relevant medical system knowledge for all, negating the one technique that fits all expertise.

5. Conclusions

Over the past decade, information security based on cognitive intelligence approaches and techniques has been a popular studied topic, which is widely used to satisfy the growing demand for reliable and intellectual systems. This paper extensively analyzed ANN, ECI methods and strategies for information security in cognitive intelligence. More journals and conference papers revealed in the recent decade on information security have been reviewed. These papers have been regarded and analyzed according to the concepts used in cognitive intelligence and its application areas. In addition, the present challenges of information security approaches to cognitive intelligence have been discussed. At present, approaches to cognitive intelligence have been widely used in the related to information security and have produced successful results. As more and more scenarios/systems need information security in the future, it is important to develop more sophisticated methods and techniques for cognitive intelligence. We predicted that ANN and ECI approaches to cognitive intelligence would persist to be urbanized and its information security applications would continue to be extended. We anticipate that scholars interested in this field will benefit from this survey. Our future research will concentrate on a more detailed study of information security approaches to cognitive intelligence.

Conflict of interest

The authors have no conflict of interest to declare.

Financing

The authors received no specific funding for this work.

References

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370. https://doi.org/10.1007/s10845-012-0683-0

Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

Cao, K., Yang, X., Chen, X., Zang, Y., Liang, J., & Tian, J. (2012). A novel ant colony optimization algorithm for large-distorted fingerprint matching. *Pattern Recognition, 45*(1), 151-161. https://doi.org/10.1016/j.patcog.2011.04.016

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28-46. https://doi.org/10.1287/isre.1050.0041

Choudhary, A. K., & Swarup, A. (2009). Neural network approach for intrusion detection. *Proceedings of the 2nd International Conference on Interaction Sciences Information Technology, Culture and Human - ICIS '09*. https://doi.org/10.1145/1655925.1656163

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of management information systems, 31*(2), 285-318. https://doi.org/10.2753/MIS0742-1222310210

El-Alfy, E. S. M., & Awad, W. (2016). Computational intelligence paradigms: An overview. *Improving Information Security Practices through Computational Intelligence*, 1-27. https://doi.org/10.4018/978-1-4666-9426-2.ch001

Iqbal, R., Doctor, F., More, B., Mahmud, S., & Yousuf, U. (2020). Big data analytics: Computational intelligence techniques and application areas. *Technological Forecasting and Social Change, 153*, 119253. https://doi.org/10.1016/j.techfore.2018.03.024

Junaid, T., Sumathi, D., Sasikumar, A. N., Suthir, S., Manikandan, J., Khilar, R., ... & Raju, M. J. (2022). A comparative analysis of transformer-based models for figurative language classification. *Computers and Electrical Engineering, 101*, 108051. https://doi.org/10.1016/j.compeleceng.2022.108051

Kulkarni, R. V., Förster, A., & Venayagamoorthy, G. K. (2010). Computational intelligence in wireless sensor networks: A survey. *IEEE communications surveys & tutorials, 13*(1), 68-96. https://doi.org/10.1109/SURV.2011.040310.00002

Kumar, H. (2018). Computational intelligence approach for flow shop scheduling problem. In *Handbook of Research on Emergent Applications of Optimization Algorithms* (pp. 298-313). IGI Global. https://doi.org/10.4018/978-1-5225-2990-3.ch013

Siddique, N., & Adeli, H. (2013). Computational intelligence: synergies of fuzzy logic, neural networks and evolutionary computing. John Wiley & Sons.

Sonawane, S., Karsoliya, S., Saurabh, P., & Verma, B. (2012). Self-configuring intrusion detection system. In *2012 Fourth International Conference on Computational Intelligence and Communication Networks* (pp. 757-761). IEEE.
https://doi.org/10.1109/CICN.2012.181

Suthir, S., & Janakiraman, S. (2018). SNT algorithm and DCS protocols coalesced a contemporary hasty file sharing with network coding influence. Journal of Engineering Research, 6(3).

Suthir, S., Janakiraman, S., Srividya, M., & Anusha, N. (2016). 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) (pp. 673-676). IEEE.
https://doi.org/10.1109/AEEICB.2016.7538376

Tao, M., Ota, K., & Dong, M. (2018). Locating compromised data sources in IoT-enabled smart cities: A great-alternative-region-based approach. *IEEE Transactions on Industrial Informatics, 14*(6), 2579-2587.
https://doi.org/10.1109/TII.2018.2791941

Thaler, S., Menkovski, V., & Petkovic, M. (2018). Deep learning in information security. *arXiv preprint arXiv*:1809.04332.
https://doi.org/10.48550/arXiv.1809.04332

Wu, S. X., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: *A review. Applied soft computing, 10*(1), 1-35.
https://doi.org/10.1016/j.asoc.2009.06.019

Yakura, H., Shinozaki, S., Nishimura, R., Oyama, Y., & Sakuma, J. (2018). Malware analysis of imaged binary samples by convolutional neural network with attention mechanism. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy* (pp. 127-134).
https://doi.org/10.1145/3176258.3176335

Yang, J., & Eickhoff, C. (2018). Unsupervised learning of parsimonious general-purpose embeddings for user and location modeling. *ACM Transactions on Information Systems (TOIS), 36*(3), 1-33.
https://doi.org/10.1145/3182165

Yang, J., & Eickhoff, C. (2018). Unsupervised learning of parsimonious general-purpose embeddings for user and location modeling. *ACM Transactions on Information Systems (TOIS), 36*(3), 1-33.
https://doi.org/10.1145/3182165