Information Protection in Cognitive Science

Shahid Naseem, Khalil Ahmed

National College of Business Administration & Economics, Lahore, Pakistan

Abstract

Expert systems being computer systems emulate the decision-making ability of a human expert, these systems have also enable a human to monitor and control security related issues in individual or distributed environment. In these systems encryption techniques are used to secure precious information with objectives such as reduce space requirements for data storage and time for data transmission. In these systems, artificial intelligence supports real-time analysis of security threats. The drawback of encryption techniques is that, the algorithm of encryption techniques may contain some loopholes, which may cause to exploit the information security by an intruder and may damage very sensitive data. To overcome the classical encryption techniques problems, cognitive science has become the inspiration in terms of human-like rationality in decision making and logical functionality. In cognitive science, it is exposed that human mind is not applying any encryption for security purposes, instead, it is using a combination of various cognitive correlates such as intention, perception, motivation and emotions as security and secrecy phenomenon. In cognitive science, it is more appropriate to elaborate cognitive memory functions to attain human like information protection and manipulation for AGI-agents. In this paper, we will discuss cognitive memory functions to attain human-like information protection and manipulation for AGI-agents.

Key Words:

Expert systems, encryption techniques, AGI-agents, sensitivity, effectiveness, emotions, motivation.

1. Introduction

The expert systems support the human to monitor the security related issues in real-time in a network environment. These systems are capable to analyze the malicious data and secure the data in real-time (Mariana, 2007). In these systems, artificial intelligence supports investigation of malicious data in real-time which helps an expert system to prevent intrusion at the initial stage. Artificial intelligence is also helpful to reduce the obliteration caused by the intruders as well as to reduce the risks of losing data during communication from one module to another module [1]. The expert systems require a security event management approach having real-time analysis capabilities, adaption and visualization to predict possible attacks on human actions.

Network security system relies on multiple components such as network monitoring, security software, hardware and applications for data protection purpose. In network security system cryptography techniques are used for data protection. In expert systems, encryption techniques are used to reduce space requirements for data storage and time for data transmission. Encryption techniques are also used to change the text format of the data to be forwarded to the receiving end so that it cannot read by an intruder. Encryption key may be in the form of alphabetic, numeric or alpha-numeric [2].

In encryption techniques, content data would be used as input data so that the data become unreadable for attackers. In these techniques, one node needs to communicate with another node, therefore, public and private keys are used for encrypting and decrypting data in a network [3]. Public key is used to encrypt the data before sharing it with the receiver. At receiver end, when encrypted message is received, a private key is used to decipher the message [4].

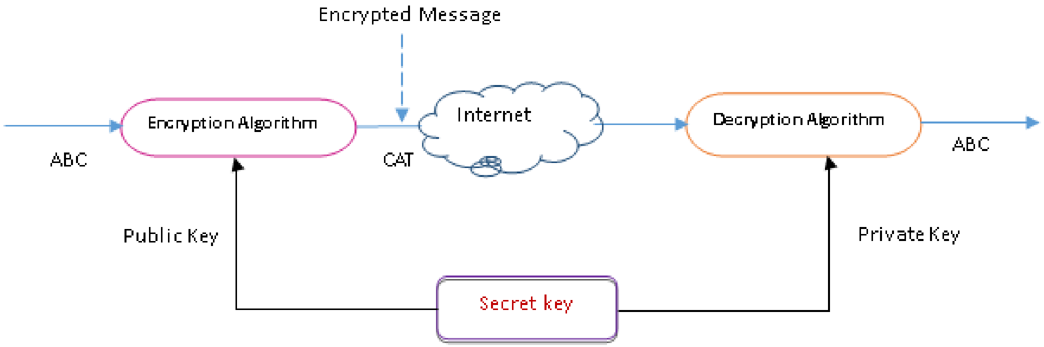


Figure 1: Classical Encryption/Decryption Techniques

Manuscript received March 5, 2017
Manuscript revised March 20, 2017

Figure 1 shows that a sender generates a message ABC over internet and send it to the receiver. The public encryption key is used at the sender end to encrypt the message before sharing it over the internet. Due to the public and private keys, the content of the message will not be compromised by an intruder during communication without private key. The figure also shows that a private key is being used at the receiving end to decrypt the message.

In expert systems, another technique that is used for protecting the data is quantum encryption. In quantum systems, the security measures are much higher than the classical systems but it lacks the flexibility that conventional cryptographic systems can provide. Quantum computation can be used more consistently for modelling, optimization and cryptography purposes due to its broad range of experimental observations. Quantum encryption technique is used to overcome the problems of classical encryption techniques such as memory size, speed and accuracy. In quantum encryption technique, public key is used to encrypt the photonic message before sharing it over the internet and private key to decrypt the photonic message [5].

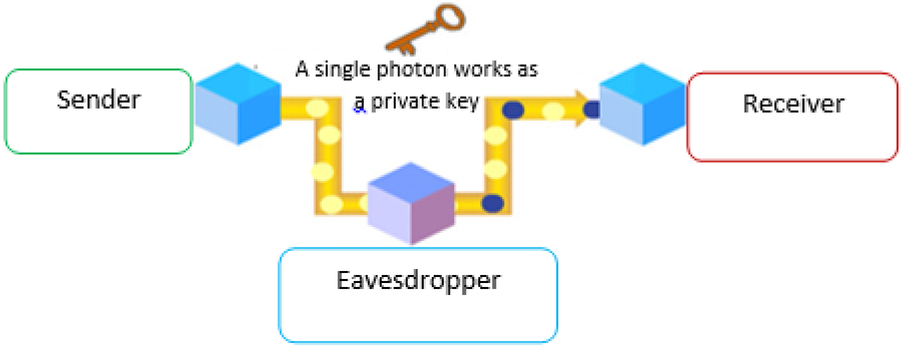


Figure 2: Quantum Cryptography

Figure 2 shows that a sender sends a photon packet to receiver after encrypting the message using a public encryption key, but during the transmission of photon packet, in the middle the packet is received by an eavesdropper and may change the entanglement state of the photonic data. When the receiver receives the packet, due to the entanglement disturbance, the presence of an eavesdropper will be exposed.

In quantum computation, privacy is a prominently strong feature, as no data is lost even if an eavesdropper analyzes the data. Therefore, in quantum computation, the sender and receiver must adopt an authenticated channel for data communication, both sender and receiver must have previous communication record for using the encryption key in a secure manner [6].

Classical encryption techniques may assure the secure communication for a certain timeframe as it is a matter of time for intruders to understand the loopholes in the algorithm which always keeps the risk high on data damage at rest or in transition. On the other hand, in quantum systems, quantum encryption techniques cannot assure the secure communication of a photon packet between a sender and a receiver as in these techniques, quantum key distribution may cause channel losses during the qubits communications. Another common aspect

2. Literature Review

In networks, cryptography is used to protect the network as well as data transmission over wireless or wire-based networks. In wireless network, cryptography relies on layers of protection and multiple components such as networking monitoring and security software in addition to hardware and appliances [7].

Simmonds proposed a network security system for monitoring network resources. In the proposed security system, they have defined the policies for monitoring data attacks, modify the data or denial of services in computer networks (Simmonds, Sandilands & Van, 2004). In neural networks, content data is used as an input data for cryptography so that data become unreadable for attackers and remains secure from them. In neural networks, algorithm can be used as public-key encryption, hashing or generation of pseudo-random numbers. Cryptography can be used to hide message information and making it unintelligible to any unauthorized party, it can also be used for encrypting the normal text message into coded text or cipher text [7].

In distributed networks, key technologies that are adopted by the network such as network equipment, automated scanning and analysis techniques are utilized for realizing system vulnerability analysis [8].

Artificial Intelligence techniques such as machine learning, training an artificial agent detector are being used to secure data by tackling security problems such as capturing a particular malicious activity in the web applications. An automated protection mechanism might bounce suspicious emails that appear to come from friends and send re-send request to friends using email address from the recipient's contact list. Artificial Intelligence techniques are used to predict the user's vulnerability to social engineering attacks [9]. Russell proposed artificial intelligence based system that could think like a human. According to this paper, cognitive science can be used as human mind to store the information and to perform highly complicated tasks [10]. In 2008, Hong proposed artificial intelligence systems for detecting and dealing with information attackers and intruders in living organisms due to its capability of adaptability and dynamic learning [11].

Chen proposed NeuroNet to collect and process distributed data, coordinate the activities within the network, analyze the irregularities, make alerts and counter measures. This research highlights NeuroNet as more effective against the denial of services attacks [12].

In 2010, Rui proposed an information security system, in which they used artificial intelligence for analyzing the unknown information attacks. According to them, the information security system has capability to receive the information patterns from external environment, adapt it and then make decision on the heterogeneous data more efficiently [13].

3. Cognitive Science and Security Measures

In cognitive sciences, an information protection agent addresses the association between correlates such as emotions and motivations that can provide security for memory management as in human-mind. The information protection agent will protect the information before sharing it to other agents within the system. The information protection agent will share the sensitive information to other agents on the basis of trust and expectation after categorizing the information on the basis of sensitivity and effectiveness i.e. less sensitive less effective, less sensitive more effective, more sensitive less effective and more sensitive more effective. The information protection agent will share sensitive information to other agents without classical or quantum encryption that are being used to secure data in digital systems.

In recent past, much of information security research and analysis have been focused on technical solutions and not on the human cognitive factors. In this paper, we have focused on the human factors such as perception, intention, motivation and emotions for understanding the information security issues.

In cognitive science, human factors such as motivation and emotions are responsible to identify the processes that are related to the past experiences. Cognitive science is also used to infer the people's mental states as well as their pre-dispositions to particular behavior [14]. In cognitive science, security measure is a condition perceived or confirmed of an individual, a community, an organization, an institution or a state to protect threats in the country such as terrorism or other deliberate or hostile situations. Cognitive science differentiates the concept of human nature, and mechanisms of human motivation and behavior. Artificial intelligence itself is not a cognitive process but it can be used to run synthetic cognitive processes. Cognitive science is used to develop such agents which may have capabilities of thinking, learning and decision making like a human [15]. The cognitive agent may have a deficiency of rationality and weakness in managing the behavioral changes. Due to these deficiencies, a cognitive agent is not able to make its own decision in critical situations (Franklin, 2007).

In a cognitive agent, human-like capabilities can play an import role to acquire new skills and new knowledge for analyzing behavior of the other agents. Cognitive science may provide the human-like behavior in a cognitive agent such as ability to think, learn by examples, doubt, act, see and speak to the computer elements [16]. Cognitive science can work as human-like behavior machine and can provide a platform for solving a wide range of complex problems of information security systems.

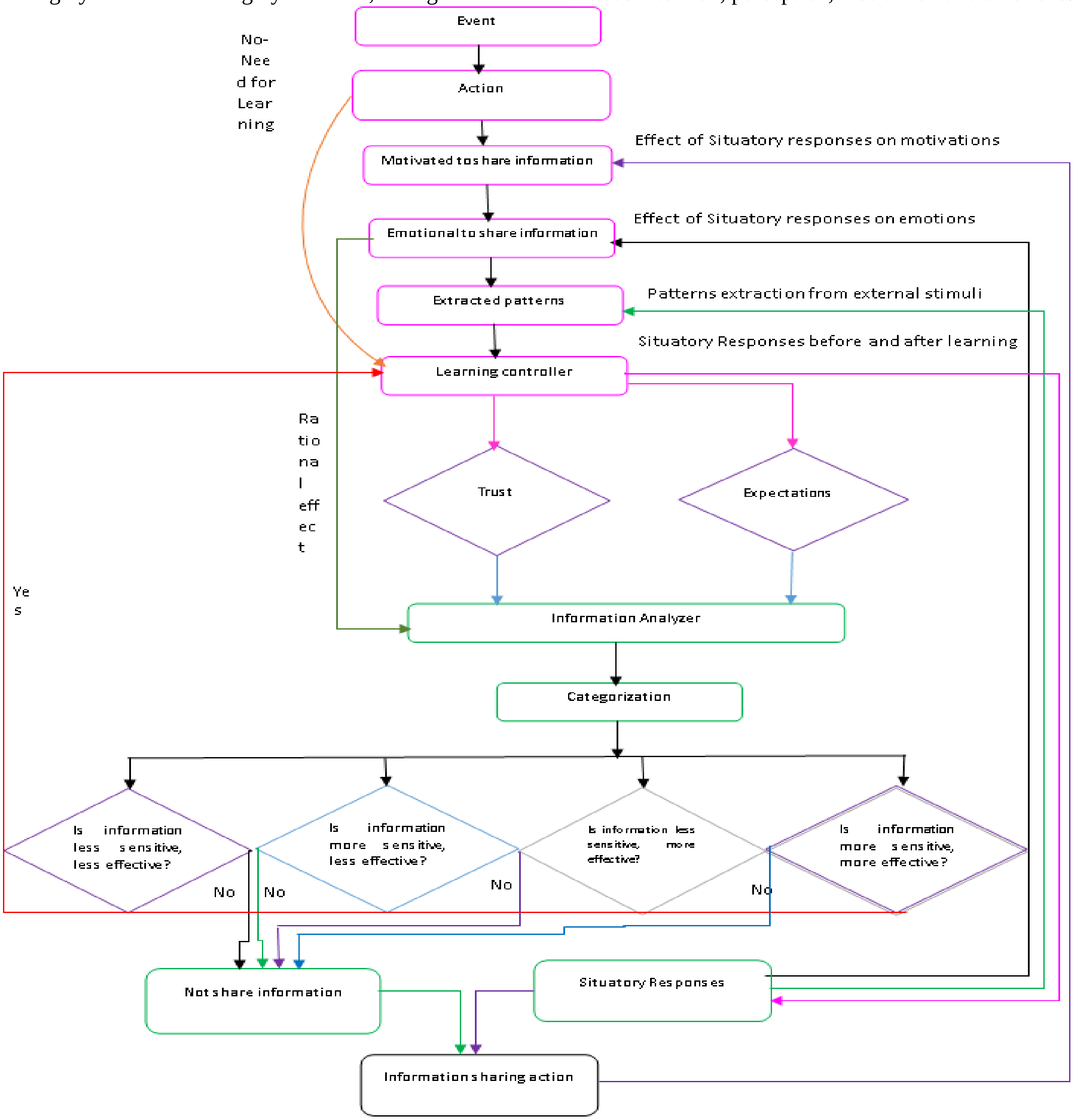
A. Methodology

To attain an autonomous privacy and security for memory management, in this paper, we have proposed a self-information protection agent for protecting sensitive information before sharing to other agents within the architecture. Our proposed self-information protection agent consists of sub-modules such as action, motivation, emotions, learning controller, information analyzer and information sharing decision modules. All these modules communicate with each other to protect the information before sharing it to other agents.

In self-information protection agent, the action module will receive the information patterns about events occurred in the external environment, it will check either the received information patterns from external environment require learning or not. If these patterns require learning for further processing then the action module will forward these patterns to the learning controller module for processing to the situatory response module for generating responses. During this process information analyzer starts evaluating the trust and expectation level of the other agents with whom information is going to be shared. On the other hand, it will forward the information patterns to check the behavior of the information protection agent i.e. the motivation and emotions of the agent for protecting the information before sharing it to Situatory responding module.

After analyzing the trust and expectation level, the categorization module will analyze the sensitivity and effectiveness level of the information patterns. If an information is less sensitive and less effective, then the information protection agent will forward this information to not sharing module. If information is highly sensitive and less effective, then the agent will process this information to information sharing module. If an information that is less sensitive and highly effective the agent will keep this information in its memory for later use. If an information that is highly sensitive and highly effective, the agent will process this to information sharing module to check the trust and expectation of the agent with whom the sensitive information is decided to be shared.

The situatory response agent does not encrypt any message before sharing it to security module for analyzing the appropriate behavior of the agent, instead, this module will process generated responses for analyzing the information sharing agent's rational behavior for taking an action i.e. information protection before sharing it to other modules within the architecture on the basis of cognitive correlates such as intention, perception, motivation and emotions.


Event
Action
No-Need for Learning
Motivated to share information
Effect of Situatory responses on motivations
Emotional to share information
Effect of Situatory responses on emotions
Extracted patterns
Patterns extraction from external stimuli
Situatory Responses before and after learning
Learning controller
Rational effect
Trust
Expectations
Yes
Information Analyzer
Categorization
Is information less sensitive, less effective?
Is information more sensitive, less effective?
Is information less sensitive, more effective?
Is information more sensitive, more effective?
No
No
No
No
Not share information
Situatory Responses
Information sharing action

Self-information protection in memory management

4. Conclusion

Conventional digital systems are using various encryption techniques such as classical encryption technique and quantum encryption technique to automatically protect the information. In this paper, we have proposed a self-information protection agent which is an advanced level of quantum encryption technique. Cognitive science has become the inspiration for artificial intelligence in terms of human-like rationality in decision making and logical functionality. As in cognitive science, human mind is not applying any encryption for the security purposes, instead, it is the combination of various cognitive correlates such as intension, perception, motivation and emotions which are generating security and secrecy phenomenon to attain human-like information protection and manipulation for artificial general intelligence-agent.

Our proposed self-information protection agent contains motivation, emotions and learning for protecting the sensitive information before sharing it to other agents. In the information protection architecture, the cognitive factors such as motivation, emotions, and categorization, trust and expectation modules communicate with each other for protecting the information before sharing it to other agents. Our proposed self-information protection agent will be used for positive association between extroversion and the level of sharing sensitive information for security purposes. The proposed self-information protection agent will categorize the information into four categories on the basis of its sensitivity and its effectiveness i.e. less sensitive less effective, less sensitive more effective, more sensitive less effective and more sensitive more effective before sharing it to other agents. The self-information protection agent analyzes the trust and expectation level on the other agents before sharing the sensitive information to these agents.

Reference

[1] J. Giarratano and G. Riley, Expert Systems principles and programming, Boston Massachusetts: PWS-KENT, 1989.

[2] S. Ajit and G. Rimple, "Data Security using Private Key Encryption System based on arithmetic coding," International Journal of Network Security & its Applications, 2011.

[3] V. Jennifer, "Secrutiy Data in Transit," LDP standards, 2002.

[4] K. Avi, "Classical Encryption Techniques for Computer and Network Security," Avinash Kak Purdue University, 19 April 2015.

[5] M. Tim, "Quantum Computing and Cryptography," January 2009. [Online].

[6] J. Barrett, L. Hardy and A. Kent, "No signaling and Quantum key distribution," Physical Review Letters, p. 95(1), 2005.

[7] N. Kumar, "Review on Network Security and Cryptography," International Transaction of Electrical and Computer Engineers System, pp. 1-11, 2015.

[8] L. Song, "Research of key technical issues based on computer forensic legal expert system," international Symposium & Informatics, 2015.

[9] C. David, C. Dan, H. Deniel, K. Jon and S. siddharth, "Feedback Effects between Similarity and Social Influence in Online Communities," KDD, 2008.

[10] S. J. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, New Jersey: Prentice Gall, 2010.

[11] L. Hong, "Artificial Immune System for Anomaly Detection," in IEEE International Symposium on Knowledge Acquisition and Modeling Workshop, 2008.

[12] Y. Chen, "NeuroNet: Towards an Intelligent Internet Infrastructure," in 5th IEEE Consumer Communications and Networking Conference, 2008.

[13] L. Rui and L. Wanbo, "Intrusion Response Model based on AIS," in International Forum on Information Technolgoy and Applications, 2010.

[14] F. Thomas, "Ethical issues in neuroscience," 2008.

[15] C. Pennachin and B. Goertzel, "Contemporary Approaches to Artificial General Intelligence," in Artificial General Intelligence, Berlin, Springer Berlin Heidelberg, 2007, p. 30.

[16] D. Vernon, "Enaction as a Conceptual Framework for Developmental Cognitive Robotics," PALADYN Journal of Behavioral Robotics, p. 10, 2010.

[17] S. Franklin, "A Foundational Architecture for Artificial General Intelligence," in Proceedings of the 2007 conference on Advances in Artifical general Intelligenc: Concept, Architectures and Algorithms: Proceeedings of the AGI Workshop 2006, Amsterdam, 2007.

[18] W. Duch, R. J. Oentaryo and M. Pasquier, "Cognitive Architectures: Where do we go from here?," AGI, Vol. 171IOS Press, p. 15, 2008.

[19] G. Alexander and M. Raul, "Advanced in Artificial Intelligence Applications," Center for Computing Research, 2005.

[20] A. A. Abdel-Fattah, T. R. Besold, H. Gust, U. Lrumnack, M. Schmidt, K.-U. Kuhnberger and P. Wang, "Rationality-Guided AGI as cognitive systems," in In proceeding of: Proc. of the 34th annual meeting of the cognitive science society, Sapporo, 2012.

[21] C. Ullrich and A. Chen, "An easily implementable method to support goal-directed learning," in proceedings of the world conference on educational multimedia, hypermedia & telecommunications, Lugano, 2004.

[22] O. Markic, "RATIONALITY AND EMOTIONS IN DECISION MAKING," Interdisciplinary Description of Complex Systems, p. 11, 2009.

[23] B. Max and D. Vladan, "Intelligence Applications and Innovations," in 18th IFIP World Computer Congress, 2004.

[24] B. Jamal, T. Francesa, J. C. Jhen and L. Jihad, "A security Framework for agent-basd systems," CitiSeeers, 2007.

[25] L. Ondrej, T. Mollmer and M. Manic, "Neural Network Based Intrustion Detection System for Critical Infrastructures.," in Proceedings of International Joint Conference on Neural Networks, 2009.

[26] C. Bitter, A. David , Elizondo and T. Watson, "Application of Artificial Neural Network and related techniques to intrusion detection," in The 2010 International Joint Conference on Neural Networks (IJCNN), Barcelona, 2010.

[27] C. Liu, J. Yang, Y. Zhang, R. Chen and J. Zeng, "Research on Immunity-based Intrusion Detection Technology for the

Internet of Things," in 7th International Conference on Natural Computation vol.1, 2011.

[28] S. Kumar, "Review on Network Security and Cryptography," International Transaction of Electrical and Computer Engineering System, pp. 1-11, 2015.