

Cognitive Informatics (CI) and Cognitive Computing (CC): A steps towards Integrating Cyber Security & IoT



Dr. Subodh Kesharwani

Being the founding editor, it is our moral duty to bring into line the piece of writing and raise symmetry so that same can be contented to readers by a large. The 4th edition in the form of Volume-1 Issue-4, Sep 2019 have recognized seven articles for this particular issue which further have been bifurcated as per there nomenclatures as and when required in a whole issue. "Anomaly Detection for Cognitive Intelligence" falls under Experimental research paper and three papers, "The Cyber security Challenge in the Age of Digital Transformation", "Growing Threat of Cyber Crime in Indian Banking Sector" and "Geospatial Services as SAAS: Trends and Drivers" falls under – Argument based credentials. On the other hand, we had one study which talks about Strategy for adopting 5G in Enterprise and two scrutiny tips (ST) "Data-Driven Security for the Organisation" and "IoT Deployment & Security Aspects". All these papers are well structured and going to facilitate the readers and enhance their knowledge bank.

Research is a long-term territory with importunate and focused efforts lead to optimistic results. When research is done in the field of Cyber vis-à-vis its economics, it has a plentiful collide and connotation not only for the corporate world but also for academia. Fostering Cyber research and providing a platform to publish good quality research papers based on empirical or scholarly research work has been an incessant endeavor of CYBERNOMICS.

I am truly honored to have been selected as the new Editor of the new monthly periodical Cybernomics. I am also very proud to be working in tandem with an outstanding team of Associate Editors and members of the Editorial Board. The latter have been selected as a balanced global illustration of the guidance in our turf. This is an editorial team that is fully engaged and committed to the success of these outstanding periodicals.

In this new era of Cyber there are a number of changes that we would like to highlight to the periodical's readers, as we are self-assured such changes will plead to an extensive range of academic and information technology interests. First, our periodical is a debut edition that has been collectively designed by our leadership team that aims to represent the global network of our community from cyber society. We recognize the importance of ensuring that our initiatives in an academic format would represents the work and research being conducted in all regions of the world, and at the same time also highlights key issues critical to technocrats not only in developed countries but also in low-resource countries. Second, the periodical will feature original articles that showcase important issues related to cyber and burgeoning terms which revolves around it.

Keywords: Artificial Intelligence, Brain-Inspired Systems, Cognitive Computers, Cognitive Engineering, Cognitive Informatics, Cognitive Robotics, Cognitive Systems, Computational Intelligence, CWW, Deep Learning, Deep Reasoning, Deep Thinking, Denotational Mathematics, Knowledge Learning



Source: <https://www.peerbits.com/blog/difference-between-m2m-and-iiot.html>

By 21 century, it is predictable that the quantity of associated devices is humdrum to cultivate exponentially to 50 billion. The main driver for this augmentation is not human populace; to a certain extent, the fact that devices we use every day (e.g., refrigerators, cars, fans, lights) and operational technologies such as those found on the factory floor are becoming connected entities across the sphere. This world of interconnected things where the humans are interacting with the machines and machines are talking with other machines (M2M) — area this time and it is at this chance to hang about. The Internet of Things (IoT) can be defined as "an ambient and universal network which enables monitoring and have power over of the physical environment by collecting, processing, and analyzing the data generated by sensors or smart objects."

From the above mentioned figure it is well versed that connectivity both M2M and IOT (Internet of things) provide allows for the collection of analytics and other valuable insights that businesses can use to leverage in the improvement of their systems. Undeniably, M2M (machine to machine) and IoT share common aspects. The core similarity is that both provide remote access to machine data and both exchange information among machines without human interference.

The expression computational intelligence (CI) usually refers to the capability of a computer to learn a explicit task from data or experimental surveillance. Even though it is universally well thought-out a synonym of soft computing, there is still no generally accepted definition of computational intelligence. The word cognition flipside to the 15th century, when it predestined "philosophy and consideration". Consideration to cognitive processes came about more than eighteen centuries ago; on the other hand, initiate with Aristotle (384–322 BC) and his interest in the main central workings of the brain and how they influence the human know-how. Aristotle focused on cognitive areas pertaining to recollection, judgment, and psychological metaphors. He placed enormous implication on ensuring that his studies were based on empirical verification, that is, scientific information that is assembled through observation and meticulous experimentation. Two epochs later, the foundation for up-to-the-minute concepts of cognition was laid during the clarification. In the twentieth century "Cognitive security is the application of AI technologies patterned on human thought processes to detect threats and look after physical and digital systems".

Cognitive Computing vs. AI

COGNITIVE COMPUTING		ARTIFICIAL INTELLIGENCE
Machine learning, natural language processing, neural networks, deep learning, sentiment analysis	TECHNOLOGIES	Machine learning, natural language processing, neural networks, deep learning
Simulate human thought processes to assist humans in finding solutions to complex problems	CAPABILITIES	Find patterns in big data to learn and either reveal hidden information or deliver solutions to complex problems
Augment human capabilities	PURPOSE	Automate processes
Customer service, healthcare, industrial sector	INDUSTRIES	Finance, security, healthcare, retail, manufacturing, government

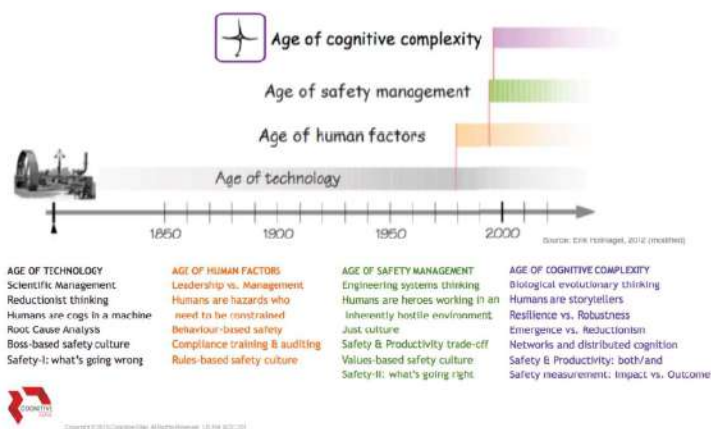
From the figure on the left it is noticeable that how cognitive technology enables AI to protect citizens. It is our accountability to put off and keep the safe public from dangers and crimes. Currently fraud recognition is a demanding predicament. But AI uses many influential techniques which tender unbeaten solutions in the area of fraud and crimes.

Although Artificial Intelligence and Computational Intelligence look for a comparable long-standing goal: reach general intelligence, which is the intelligence of a machine that could carry out any academic task that a human being can; there's a clear dissimilarity between them. According to Bezdek (1994), Computational Intelligence is a subset of Artificial Intelligence. There are two types of machine intelligence: the artificial one based on hard computing techniques and the computational one based on soft computing methods, which facilitate altered copy to numerous situations.

CI and CC are fields not only for basic studies on the brain, computational intelligence theories, and denotational mathematics, but also for engineering applications in cognitive systems towards deep learning, deep thinking, and deep reasoning.

Like other cognitive computing applications, self-learning security systems use data mining, pattern recognition and natural language processing to simulate the human brain, albeit in a high-powered computer model. Such automated security systems that are premeditated to solve problems without requiring human resources. Cognitive safety measures may be principally cooperative as a technique to put off cyber-attacks that engineer human discernment. Such attacks, sometimes referred as cognitive hacking, are designed to affect people's behaviors in a way that serves the attackers purpose.

Evolution of safety



Cognitive security efforts in this area take account of non-technical approaches to make individuals less vulnerable to manipulation as well as technical solutions designed to detect misleading data and disinformation and prevent its dissemination. Humans are commonly seen as the weakest link in corporate information security. This leads to a lot of effort being put into security training and awareness campaigns.

$$\text{Cybersecurity Risk} = \frac{\text{Threat Level} \times \text{Probability of Attack} \times \text{Points of Exposure}}{\text{Cybersecurity Measures Implemented}}$$

Source: based on the above equation for the level of cyber security risk from Bosch

The approaching business outside edge that admittance to data from billions of connected devices offers is too much for enterprises to refuse to go along with. As a result, in 2019 increasingly enterprises will be connected to the Internet of Things (IoT) using more and more endpoints. It's not all good despite the fact that, all those endpoints mean more assault vectors for hackers to take gain of vulnerabilities are threatening to tear down trust in the connected world, especially as IoT moves into B2B spaces and industrial sectors where risks are much higher. With data security a dominant anxiety for enterprises, security will take preference over innovation if confidence in IoT is to cultivate and ruthless security issues are to be avoided. If this can be finished, it is probable that adoption will persist at an exponential rate, greater consolidation will coerce developers to edge computing and connected applications will unlock multipurpose robots, leading to far greater capability and functionality.

The concepts and technologies that have demonstrate the technique to the IoT, or the interconnectivity of real-world objects, have existed for some instantaneous. Many people have referred to Machine-to-Machine (M2M) communications and IoT interchangeably and think about them one and the counterpart. In truth, M2M can be viewed as a subset of the IoT. The IoT is a more encompassing phenomenon, which includes Machine-to-Human communication (M2H), Radio Frequency Identification (RFID), Location-Based Services (LBS), Lab-on-a-Chip (LOC) sensors, Augmented Reality (AR), robotics and vehicle telematics. Many of these technologies are the result of developments in military and industrial supply chain applications; their common feature is to combine embedded sensory objects with communication intelligence, running data over a mix of wired and wireless networks. In a broader context, the architecture encompasses the Internet of Things plus business engineering insights captured from the information transmitted by these so-called "smart objects." The focal point and competence of this editorial thought is wholly on the security aspects of the Internet of Things and make reader aware about how modern technology is knocking a door.

Thus Data driven security refers to using quantifiable factors to coerce a security program. While not all elements of a security program provide themselves to dimension, many components can be measured successfully. A frequently established business paradigm state, what cannot be measured cannot be administer. Some would disagree that the safety is more of an art than knowledge. While they are accurate, the business of security is not a talent.

Research is a long-term territory with importunate and focused efforts lead to optimistic results. When research is done in the field of Cyber vis-à-vis its economics, it has a plentiful collide and connotation not only for the corporate world but also for academia. Fostering Cyber research and providing a platform to publish good quality research papers based on empirical or scholarly research work has been an incessant endeavor of CYBERNOMICS.

We are truly honoured to have been selected as the new Managing Editors of the new monthly periodical Cybernomics. We are also very proud to be working in tandem with an outstanding team of Associate Editors and members of the Editorial Board. The latter have been selected as a balanced global illustration of the guidance in our turf. This is an editorial team that is fully engaged and committed to the success of these outstanding periodicals.

In this new era of Cyber there are a number of changes that we would like to highlight to the periodical's readers, as we are self-assured such changes will plead to an extensive range of academic and information technology interests. First, our periodical is a debut edition that has been collectively designed by our leadership team that aims to represent the global network of our community from cyber society. We recognize the importance of ensuring that our initiatives in an academic format would represents the work and research being conducted in all regions of the world, and at the same time also highlights key issues critical to technocrats not only in developed countries but also in low-resource countries. Second, the periodical will feature original articles that showcase important issues related to cyber and burgeoning terms which revolves around it.

The response to our appeal to authors for contribution has been overwhelming. In spite of our preminent efforts, due to an assessment of editorial board and the referee review board, some of the articles/papers could not be incorporated in the present debut issue, but this shall not put a ceiling on any of the authors to send their original articles, case studies, research reviews or empirical contributions for publication in our periodical.

As managing editors, we recognize the value authors place on high-quality and unbiased peer review conducted in an appropriate manner. In totaling, we value the significance of rapid publication, and so to that end we have structured our editorial team to comprise Associate Editors, a Social Media Editor, and a Video Editor so we are capable to

expedite the processing of submitted manuscripts. We have instructed all those involved with the periodical in an attempt to endow with the highest standard of manuscript review, editing, and publishing. We have implemented rigorous peer review criteria, and this will be reflected in the quality of published articles. We also want to persuade all those who are interested in being part of this energetic and enthusiastic team to contact us, as we will welcome your contribution. We invite colleagues working in related disciplines of cyber and information technology as an appropriate medium for the publication of your own high-quality research.

Manuscript submissions are being accepted for Volume-1, Issue-2, May 2019 which will be in the regular format. Original articles can be submitted to the Managing Editor (Word document, by email only, at scholastic.seed@gmail.com). Articles for columns should be arranged with the respective column editor. *Cybernomics* is a right platform for academicians, industry executives, researchers and students for sharing the views and the news of the management in terms of research papers, articles and case analysis, reviews etc.

We are firm about the ensuing issues of the periodical with regard to quality and coverage. We hope that within short time this periodical will make the academicians, industry executives, researchers and students to travel from the point of recognizing something to acknowledge the whole thing. We wish the periodicals for its effort and continuity of its tempo in the same direction in the days to come. Our sincere thanks to all the contributors for their support and interest. We once again request all academicians and researchers to send their unpublished articles/papers for publication in our periodical to understand the economics of Cyber.



Dr Subodh Kesharwani

Associate Professor, SOMS, IGNOU

Subodh Kesharwani is an academician with a bronze medal in his Post graduate and Doctorate in ERP System in 2002 from Allahabad Central University. He is one of the researchers who had concentrated his research on Total Cost of Ownership [TCO] & critically evaluate ERP vendors including SAP. Dr. Kesharwani is presently an Associate Professor, School of Management Studies with a total 20 years of hardcore teaching and research in Information System and its linkages with various domains of management at Indira Gandhi National Open University, New Delhi. He is presently an expert in various burgeoning areas and had delivered a talk as a trainer on MOOCs, Team Building, E-commerce, Technology Enabled Learning, E-resource, Technology Uses in research, Block chain, Internet of Thing, Enterprise Information System, Free & Open Source Software, etc. Dr. Subodh had developed and coordinated a program in Entrepreneurship & Business Skills in collaboration with Rajiv Gandhi Foundation (RGF), India and Commonwealth of Learning, Vancouver, Canada which provides training to the trainers at IGNOU. He is presently a program coordinator of IGNOU-ICWAI alliance. He is also a founder Editor-in-chief of a peer reviewed refereed journal entitled "Global Journal of Enterprise Information System [GJEIS] from 2009 onwards, which has completed its 10 years term and published 40 issues till date both in printable and virtual format. The Journal GJEIS is equipped with DOI from Crossref USA and listed in almost 50 directories in the world with an impact factor of 2.68 of 2017-18. Dr. Kesharwani had participated as a debater in diverse TV show and participates in Interactive Radio Counseling including Gyanvani and Gyandarsshan. He had written a Book entitled "ENTERPRISE INFORMATION SYSTEMS-Contemporary Trends and Issues" in a co-authorship with Professor David L Olson (University of Nebraska, USA. which was published by WORLD SCIENTIFIC, USA. <http://www.worldscibooks.com/business/7287.html>)

He had another text book on ERP system which caters a B.Tech VI Semester CS and IT Students. He had developed educational contents for various academic Institutions such as ICAI, IGNOU and contributed articles for various journals/ Magazines, etc. He had chaired a good number of technical sessions at various conferences & seminars nationally and globally. He is presently running a "Blockchain Federation for Indian Researcher" which he thinks can bring paradigm shift holistically. Dr. Kesharwani had been awarded "IT Innovation & Excellence Award 2012" in the field of ERP solutions, by KRDWG's Selection Committee at IIT Delhi. He is in the panel of the Steering Committee of the International Journal of Computing and e-Systems, TIGERA-USA. He was in the key panel of round-table workshop conducted by Ministry of Corporate Affairs in Association with Indian Institute of Corporate Affairs to streamline "Corporate Data Management and Governance". He was one of the resource person who shared the experience with the 12 different ITEC countries participants who had attended International MDP.



Scholastic Seed Inc.

www.scholasticseed.in

Anomaly Detection for Cognitive Intelligence

– Anil Lamba

Practice Lead - Cyber Security, EXL Service Inc., NJ, USA

<https://orcid.org/0000-0002-7793-785X> dranillamba@outlook.com

Article History

Paper Nomenclature:

Experiential Research Paper (ERP)

Paper Code: CYBNMV1N4SEP2019ERP1

Submission Online: 09-Sep-2019

Manuscript Acknowledged: 10-Sep-2019

Originality Check: 14-Sep-2019

Originality Test Ratio: 6%

Peer Reviewers Comment: 24-Sep-2019

Blind Reviewers Remarks: 26-Sep-2019

Author Revert: 27-Sep-2019

Camera-Ready-Copy: 28-Sep-2019

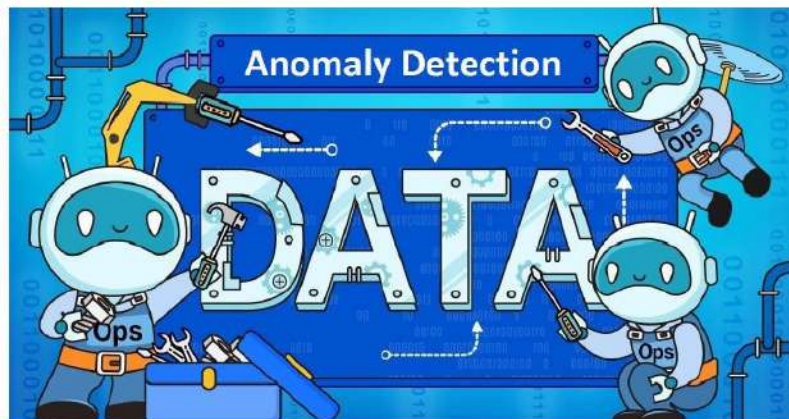
Editorial Board Citation: 30-Sep-2019

Published Online First: 2-Dec-2019

Today's industrial organizations are often tasked with objectives that are seemingly at odds with each other. They need to increase productivity while reducing machine failure or enhance product quality while speeding up time to market. Achieving these goals simultaneously can be incredibly challenging — if not impossible.

How does one work around this dilemma? The trick lies in cognitive anomaly detection and prediction, which is a process that leverages unsupervised learning (cognitive computing) and pattern recognition to quickly and accurately identify the anomalies hidden in your Industrial Internet of Things data. The use of machine learning algorithms minimizes the appearances of false alarms.

Keywords : Anomaly detection | Internet of things (IoT) | Cognitive Intelligence | Data Security



Introduction

Anomaly detection is a method used to ascertain strange patterns that do not conform to expected behavior, known as outliers. It can be used for many purposes from intrusion-detection to system-health monitoring, and from false-charges detection in credit-card transactions to Issues/fault detection in operational environments.

What Are Anomalies?

Anomalies can be broadly categorized as:

Point anomalies: A single-occurrence of data which is too far off from the rest. For-example: Identifying a credit-card fake-transaction basis "amount-spent."

Contextual anomalies: This relates when occurrences are any context-specific and usually it is common in time-bound data. For Example: Paying 50\$ on groceries every-day during the festival-season is usual, but may-be unusual otherwise.