# Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems

Habtamu Abie
Norwegian Computing Center
Oslo, Norway
habtamu.abie@nr.no

***Abstract*—Cyber Physical Systems (CPS)-Internet of Things (IoT) enabled healthcare services and infrastructures improve human life, but are vulnerable to a variety of emerging cyber-attacks. Cybersecurity specialists are finding it hard to keep pace of the increasingly sophisticated attack methods. There is a critical need for innovative cognitive cybersecurity for CPS-IoT enabled healthcare ecosystem. This paper presents a cognitive cybersecurity framework for simulating the human cognitive behaviour to anticipate and respond to new and emerging cybersecurity and privacy threats to CPS-IoT and critical infrastructure systems. It includes the conceptualisation and description of a layered architecture which combines Artificial Intelligence, cognitive methods and innovative security mechanisms.**

***Index Terms—Cognitive cybersecurity, healthcare, artificial intelligent, machine learning, cognitive techniques, CPS-IoT***

## I. INTRODUCTION

There is an increasing rich use of different types of Cyber-physical systems (CPS)-Internet of Things (IoT) applications for eHealth and welfare, ranging from provider-driven managed monitoring of humans during daily-life, to self-driven monitoring of humans, and social data aggregation and marketing. Cisco estimates that by 2020, more than 50 billion objects will be socially connected with the help of IoT and cloud technology. More recently, CPS-IoTs are being developed with the capability to learn, reason, and understand both physical and social worlds by themselves, simulating the cognitive behaviour of humans – a cognitive CPS-IoT. "In knowledge-intensive environments, the smartest uses of the IoT will be those that enable the ingrained capabilities of human thinking to take centre stage." [1]. However, all this introduces new challenges: (i) increasing cognitive complexity of CPS-IoTs can lead to unexpected emergent behaviour; (ii) cognitive CPS-IoT will suffer from traditional CPS-IoT vulnerabilities and threats [2], and new threats related to their inherent cognitive functionalities; (iii) "70% of the most commonly used IoT devices … can be hacked … 80% of these devices raised privacy concerns regarding the collection of sensitive data, e.g. for health" [3]; and (iv) CPS-IoT's ubiquity will present a significantly expanded attack surface making the public safety risks higher for critical infrastructure through its interfaces and improved flexibility of access to services and information.

Healthcare services and infrastructures are more critical, sophisticated and interconnected than ever before. While improving clinical outcomes and transforming care delivery thereby improving human life, there are, however, increasing concerns about the security of healthcare data and devices. Increasing interconnectedness has exposed medical devices and services to new cybersecurity vulnerabilities. This makes the healthcare sector the most vulnerable to major security risks. As described above, the situation is exacerbated by the CPS-IoT enabled healthcare services and infrastructures, which are vulnerable to a variety of emerging cyber-attacks. CPS-IoT systems are classified as safety and security critical systems and have characteristics of fragmentation, interconnectedness, heterogeneity, and cross-organizational nature, which present expanded attack surface. Cybersecurity attacks can potentially lead to a violation of users' privacy, physical damages, financial loses and threats to human life and preventing them is critical. Reports highlight the growth of attacks and the rise in medical identity theft with millions of medical records stolen globally [4].

The rise of cyber-physical attacks shows us that the current, security solutions are unable to tackle the dynamicity, complexity, uncertainty, and high connectivity of CPS-IoT enabled healthcare services and critical infrastructures. Cognitive architecture and artificial intelligence can enhance automated intelligent cybersecurity decision-making mechanisms with expert-level ability.

Furthermore, attackers will adapt their strategies to the security situation, and to newly deployed countermeasures. Thus, there is a critical need for innovative techniques for building cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems. This paper proposes and presents a cognitive cybersecurity methodology and theory that allow the study of the attackers' behaviour by capturing their intentions, predicting and estimating their determination and correlating these with the activity of the CPS-IoT and critical infrastructure systems to help prevent emerging attacks.

The main aim of the proposed approach is to provide a methodology for defending against dynamic and adaptive attacks to the CPS-IoT-enabled healthcare ecosystem. This will be achieved through (1) a cognitive architecture for modelling humans' cognitive behaviour to anticipate and respond to new and emerging security and privacy threats, (2) trade-offs and other contributing factors to get ahead of attackers' cognitive decision cycle accounting for uncertainties, and optimizing temporal feedback loops, (3) integrate innovative mechanisms for security, privacy, metrics, and dynamic security knowledge base to enhance threat prevention, threat detection, incident response and mitigation of impacts, (4) privacy-aware collaboration, computational techniques, adaptive data collection and actuation, and (5) integrating cross-cutting techniques such as AI predictive analytics, run-time verification, evidence collection and tracing for evidence based risk management and dynamic forensics.

## II. CHALLENGES AND MECHANISMS

Cognitive cybersecurity needs to tackle the dynamicity, complexity, uncertainty, and high connectivity of CPS-IoT enabled healthcare services and critical infrastructures to meet the challenges of the constantly evolving dynamic and adaptive attacks. Some of the multifold challenges to building a cognitive cybersecurity solution are briefly described in the next section followed by the description of innovative mechanisms for meeting these challenges.

### A. Challenges

*Cognitive cycle security model for the CPS-IoT*: It is a cognitive model with detection mechanisms and security adaptation characterized by the detection (observe & orient), planning (plan), implementation (decide & act) and learning (learn) steps. The general challenge for such architecture is how to capture at the computational level the mechanisms of human cognition, including those underlying the functions of control, learning, adaptivity, perception, decision-making, and action. The specific challenge is to design an architecture that adapts to the constraints and capabilities of the different CPS-IoTs, as well as to the possible dynamicity of these constraints and capabilities.

*Complex temporal feedback loops:* Certain activities occur at very rapid speeds requiring a very tight feedback loop to support cognitive control. Other activities occur on a longer time-scale and cognitive control algorithms may need to take into account a wider range of factors in a slow feedback loop. The correlation of cause and effect of actions is particularly challenging due to the variety of temporal loops and their dramatic speed differences [5].

*Complex interactions*: The challenge is how to capture and model many more of these interactions better than human could be capable of analysing.

*Heterogeneous intercommunications*: It is critical to solve this since heterogeneous configurations are a key enabler to dramatic improvements in network performance.

*Trade-offs and contributing factors*: The challenge is to understand the fundamental limits of the cognitive model and associated security mechanisms that can be achieved to get ahead of attackers' cognitive decision cycle accounting for uncertainties thus preventing adaptive attacks. Another challenge is the identification and better understanding of how constraints and other key control factors affect the defender-attacker cognitive process is a challenge.

*Innovative and intelligent security mechanisms*: The challenge is how to develop lightweight but effective and efficient security and privacy mechanisms for CPS-IoT and its critical components with cognitive and distributed analysis and decision making capabilities. How to integrate trust-based cognitive security that allows a more informed study of attackers' behaviour by capturing the intentions of the attackers is a challenge. Note that predicting and estimating how determined the attackers are, and correlating their background with the activity of the CPS-IoT system is a grand challenge. It requires the ability to draw inferences about others' intentions, dispositions, and actions, in order to study attacker's behaviour.

*Dynamic risks and metrics*: The challenge is how to develop adaptive metrics to map dynamic security risks to security objectives and to security metrics for validating the effectiveness of the run-time adaptivity of the security mechanisms. Adaptive attackers will adapt their strategies to the security situation and to newly deployed countermeasures. Therefore making the metrics adaptive themselves is a challenge. Furthermore, when systems grow in complexity measuring their quality is a challenging task [18].

*Integration of privacy*: The challenge is how to integrate the concept of privacy design patterns for adaptation signalling and control by analysing the atomic personal data transactions necessary for adaption into the cognitive model.

*Run-time verification*: Due to the complexity of the cognitive cycle, run-time verification is needed for guaranteeing the achievement of self-adaptive cognitive security and privacy properties. Developing verification methods for guaranteeing the achievement of self-adaptive security and privacy properties is one of the major challenges facing the entire security research field. The challenge is how to integrate lightweight run-time verification methods in a cognitive cybersecurity model for this purpose.

*Dynamic forensics*: Due to the exponentially growth of the volume of dynamic evidence collected per case, there is a need for new methods and tools built on new technologies like CPS-IoT, big data, cloud services and AI/deep learning. The challenge is how to integrate these methods and tools to capture and trace evidence dynamics effectively and reliably. It is widely accepted that "evidence dynamics is one of the perpetual challenges that commonly introduces error into forensic analysis". *Evidence Dynamics refers to any influence that changes, relocates, obscures, or obliterates physical evidence, regardless of intent* [6].

### B. Innovative Mechanisms

Cognitive cybersecurity needs innovative and intelligent mechanisms for lightweight but effective and efficient security and privacy for CPS-IoT and its critical components with the capabilities of cognitive and distributed analysis, and decision making. These must integrate trust based cognitive security that allows a more informed study of attackers' behaviour by capturing the intentions of the attackers and by predicting and estimating how determined the attackers are, and by correlating their background with the activity of the CPS-IoT system. The mechanisms must have the ability to draw inferences about others' intentions, dispositions, and actions, in order to study attacker's behaviour. They should also integrate adaptive metrics for mapping dynamic security risks to security objectives and to security metrics for validating the effectiveness of the run-time adaptivity of the security mechanisms.

The adaptive metrics must allow us to measure and adapt to adaptive attackers, which also adapt their strategies to the security situation and to newly deployed countermeasures. A combination of AI/deep learning, control theory and game theoretic modelling and analysis can be used for these purposes. Control theory can be used for attack strategy seeds, and game theory, minimax analysis, adversarial risk analysis can be used to find the optimal defender strategies.

Furthermore, the mechanisms should integrate privacy by design through model-building (data types), transaction identification (inspection of the developed adaption protocols, extraction of personally identifying (PI) computations), privacy impact analysis, formulation of design patterns (constructive approach), and evaluation through artefact design.

Finally, the application of lightweight run-time verification can be integrated for guaranteeing the achievement of self-adaptive cognitive security and privacy properties. The most important quality attributes for cybersecurity analytic systems are described in [12] and can be used to evaluate the reliability of the mechanisms and cybersecurity analytics systems. The next section describes how the combination of cognitive methods and AI help to implement these mechanisms.

## III. Artificil Intelligence for Cognitive Cybersecurity

### A. Cognitive Systems

*Cognitive systems are self-learning systems that use data mining, machine learning, natural language processing and human–computer interaction to mimic the way the human brain works. Human cognition involves real-time analysis of environment, context and intent, among many other variables that inform a person's ability to solve problems. By using cognitive systems, security trends can be analysed and enormous volumes of structured and unstructured data can be distilled into information that drives continuous security improvement* [7].

Cognitive cybersecurity, thus, aims to simulate human thinking and behaviours to anticipate and respond to new and emerging security threats, adapt constantly to changing security conditions including human participations, tasks and roles, and dynamically learn from experience and dynamic conditions. To achieve this, cognitive cybersecurity applies AI technologies patterned on human thinking processes to detect threats and protect cyber systems. These AI technologies include machine learning, deep learning, neural networks, NLP (natural language processing), sentiment analysis, etc. Self-learning security systems use these technologies to automate problem solving without requiring human resources.

It is argued that *cognitive security may be particularly helpful to prevent cyberattacks that manipulate human perception. Such attacks, sometimes referred to as cognitive hacking, are designed to affect people's behaviours in a way that serves the attacker's purpose. Cognitive security efforts in this area include non-technical approaches to making individuals less vulnerable to manipulation as well as technical solutions designed to detect misleading data and disinformation and prevent its dissemination* [8].

### B. Artificial Intelligence

*Artificial Intelligence (AI) is the branch of computer science concerned with the automation of intelligent behaviour, usually associated with human thinking such as decision making, problem solving and learning. AI techniques are appropriate for building decision-making agents that make rational actions for their given context* [5].

AI is used to identify anomalies, speed up detection, and increase the effectiveness of existing products and permit the system to train itself autonomously, at least in part (since it will require human oversight to determine the legitimacy of any alerts and gauge the correctness of AI making user feedback useful). It enables real-time, context-aware adaptivity which is required by cognitive cybersecurity systems, and enables machine learning, clustering, graph mining and entity relationship modelling to identify potential threats.

Haigh and Partridge [5] argue that certain AI techniques are more promising and/or have already produced interesting results in cognitive networking. These include Knowledge Engineering, Planning and Scheduling, Machine Learning (ML), Distributed AI and Multi-agent systems, including biologically-inspired approaches, and Game Theory. In this section, we briefly describe some of these techniques which are relevant to cognitive cybersecurity.

***Knowledge Engineering*** aims to capture knowledge for complex problems solving using ontologies, semantics and representations which are important considerations for cognitive cybersecurity.

***Machine learning algorithms*** make it possible for cognitive systems to constantly mine data for significant information and acquire knowledge through advanced analytics. Cognitive systems learn to anticipate threats and generate proactive solutions through continually refining methods and processes. This ability to process and analyse huge volumes of structured and unstructured data allows cognitive security systems to identify connections among data points and trends that would be impossible for a human to detect. Deep learning, which is the evolution of neural networks, enables the identification of complex attack patterns. ML techniques include artificial neural networks, support vector machines, clustering, explanation-based learning, induction, reinforcement learning, genetic algorithms, nearest neighbour methods, and case-based learning.

***Planning and scheduling techniques*** are appropriate for decision-making situations, where security tasks need to be organized and coordinated to meet security performance objectives, under resource constraints. In dynamic environments, the plan needs to be monitored, revised and adapted to changing conditions so as to maintain the accuracy of performance predictions. Multi-agent planning, dynamic programming, partially-observable Markov decision processes, constraint satisfaction, and distributed optimization algorithms are common techniques.

***Distributed AI and Multi-agent Systems*** are concerned with finding distributed solutions for AI problems and address domains that have the following characteristics: discrete (local goals and constraints), deprived (locally resource constrained), distributed (embedded in a physical world), decentralized (local decisions and local views of the environment with no centralized decision maker), diverse (different capabilities and different roles) and dynamic (changing task/mission and domain). These are relevant to distributed cognitive security solutions.

AI techniques are appropriate and effective solutions to meet the numerous characteristics of communications networks [5]. These characteristics are relevant to CPS-IoT enabled services and infrastructures and include:

- *Dynamic*: AI techniques for planning under uncertainty make choices that will be appropriate even as the domain changes.
- *Partially-observable*: AI techniques are good at inferring missing data and generalizing a situation so that decisions make sense for current conditions.
- *Ambiguous observations:* AI techniques are good at recognizing ambiguity or low confidence, and can either gather more information to discriminate or make decisions appropriate for both conditions.
- *Resource constrained*: AI techniques are effective at scaling a solution to the platform they are operating

on, and designing tasks that manage available resources effectively.

- *Diverse*: AI techniques consider diversity a benefit, as it allows resources to be managed in different ways.
- *Massive scale*: Data mining and ML techniques are effective even on massive datasets; moreover incremental planning and learning techniques.
- *Complex access policies*: Knowledge engineering techniques can represent policies as constraints, and then constraint reasoning techniques can find satisfying solutions quickly incorporate new information efficiently and rapidly).

Cybersecurity solutions utilizing AI and ML/deep learning can greatly reduce the amount of time needed for threat detection and incident response, and can alert anomalous behaviour in real time.

## IV. Proposed Approach

The goal of this proposed approach is the development of an integrated cognitive framework for defending against dynamic and adaptive attacks to the CPS-IoT enabled healthcare ecosystems. Thus contributing to the global cybersecurity security challenge. Achieving this goal requires an interdisciplinary approach by applying knowledge from the fields of cognitive computing, optimization, formal methods, cybersecurity, trust, forensics, artificial intelligence and mathematics.

Fig. 1 depicts the overall architecture of our cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems with the building blocks in four layers: Healthcare Stakeholders Collaboration layer, Perception and knowledge layer, Adaptive Data Collection and Actuation Layer and Healthcare Stakeholders Infrastructures layer.

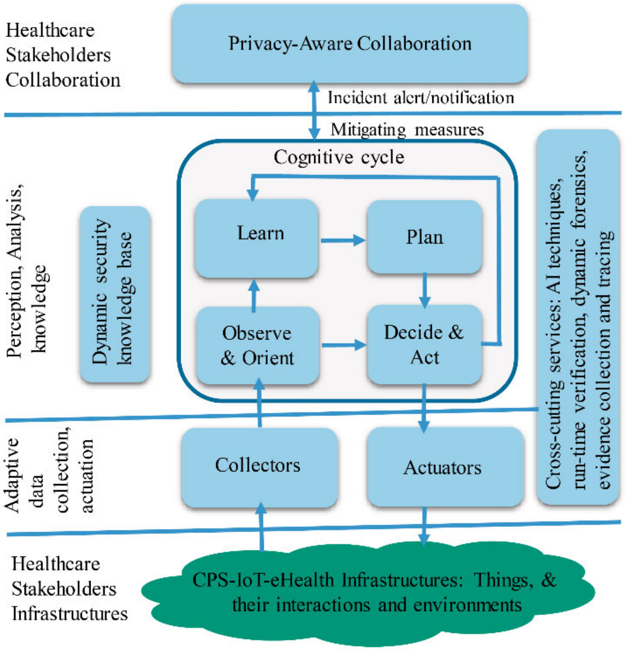
Healthcare Stakeholders Collaboration
Privacy-Aware Collaboration
Incident alert/notification
Mitigating measures
Cognitive cycle
Perception, Analysis, knowledge
Dynamic security knowledge base
Learn
Plan
Observe & Orient
Decide & Act
Cross-cutting services: AI techniques, run-time verification, dynamic forensics, evidence collection and tracing
Adaptive data collection, actuation
Collectors
Actuators
Healthcare Stakeholders Infrastructures
CPS-IoT-eHealth Infrastructures: Things, & their interactions and environments

*Figure 1 Proposed approach*

The objective of the approach is to serve as a foundation and innovative methodology for preventing dynamic and adaptive attacks to emerging smart CPS-IoT enabled healthcare environments.

The following sections briefly describe the functionality of the main building blocks at each layer.

### A. *Privacy-Aware Collaboration*

To support stakeholders to jointly refine threats and define mitigation strategies in a privacy-aware manner, a new perspective on dynamic and evidence-based risk management is required [2]. This is to highlight uncertainty and knowledge, not only probability, of complex healthcare ecosystems, which are characterized by deep uncertainties. It should provide tools for facilitating stakeholders' collaboration in a privacy preserving manner through shared situation awareness, information sharing, common reporting and visualization. Interoperability, interaction and collaboration in healthcare is primarily driven by data exchange. This brings with it new challenges and requirements around security and privacy, technology, incentives, and governance that must be addressed. Another promising solution can be a decentralized approach that uses blockchain technology to facilitate this through five mechanisms: digital access rules, data aggregation, data liquidity, patient identity, and data immutability. Blockchain technology will enhance user-centric data sharing and protect privacy through the explicit access rules enabling effective and efficient collaboration on cybersecurity and privacy at various layers of the complex healthcare ecosystems to foster cognitive cybersecurity and privacy by design.

### B. *The Cognitive Cycle Model*

The overall approach of this model is to close the cognitive cycle model, using the trade-offs, AI, controllers and innovative mechanisms, dynamically perceiving the CPS-IoT conditions and human and social environment behaviours and taking actions and learning from those actions. Feedback is possible at all stages of the loop/cycle. This will help achieve situation awareness to enhance the security adaptation to moving targets, and adversarial environments. In the literature, it has been argued that "an entity that can process this cycle more quickly than its opponent can get ahead of the opponent's decision cycle and consequently gain the advantage." [9].

The cognitive cycle security model for the CPS-IoT with detection mechanisms and security adaptation is characterized by the detection (observe & orient), planning, implementation (decide & act) and learning steps. The general challenge is how to capture at the computational level mechanisms of human cognition, including those underlying the functions of control, learning, adaptivity, perception, decision-making, and action. The more specific challenge is how the overall cognitive cybersecurity architecture adapts to the constraints and capabilities of the different CPS-IoTs, as well as to the possible dynamicity of these constraints and capabilities. It uses cognitive models of users' contexts in the physical environment in order to understand how to better support user centred privacy security and management. Cognitive models of users' human environment are also used when interacting in personal, social, public spaces and with different human stake-holders cooperating and competing with other in these spaces to maintain security and privacy. In the followings we describe the building blocks at each step in the cycle with more emphasis on Observe & Orient and Decide & Act steps.

**Observe & Orient:** At this stage the Observe phase monitors and perceives multiple stimuli. To achieve this, the Observe phase uses the adaptive data collectors such as probes/sensors at the adaptive data collection and automation layer. The **Observe** phase observes observables including factors: configuration, user activity, vulnerabilities, current threats, ongoing attacks, and interaction with the physical environment. This interaction is achieved using a range of sensing/collecting and automated auditing technologies such as configuration management, network management protocol traps, dynamic discovery tools such as nmap or traceroute, log management tools, intrusion detection systems such as Snort, automated scanners such as Nessus for vulnerability detection and develop algorithms for better fusing and aggregating sensed data from various sources in real-time [9]. Trade-offs between pulling collectors/sensors on demand and having the sensors push updates should be used for various contexts. The **Orient** phase determines the significance of an observation by analysing the meaning of the observed activities and determines the impact on the security situation in the near future. Using ontologies, a semantic approach and big data analytics strategies for optimal orientation are used due to the multitude of sensors and large amount of sensed data. Sources of sensing could also be wearables, smart phones, social media, etc. AI techniques are used to interpret these observations and identify potential factors (or root causes) of situations, to compute progress toward security performance goals, to estimate future conditions and the likelihood of achieving goals, and to decide on the urgency of responding to problems.

**Learn:** This phase learns based on perception, observation, decisions, and actions. The challenge for this stage is how to learn behaviours at human, application, and device levels so as to update models and/or knowledge for other models in other phases can make accurate predictions. It can learn environmental conditions and capabilities of adversaries using either explicit human feedback or empirical security performance data. Another challenge for this stage is how to learn faster than a possible attacker. Inverse reinforcement learning can be used in this case. In real-time learning, learning agents adapt behaviour to perform better and adapt each minute by changing strategy according to current conditions.

**Plan:** This phase generates plans and considers time reasoning by identifying goals to be achieved. Some argue that planning involves causality reasoning, conditional planning, temporal reasoning, constraint reasoning, and resource management. Multi-objective trade-offs for planning are calculated using appropriate planning techniques. In dynamic environments, the plan needs to be monitored and strategies revised so as to maintain the accuracy of the plans and adapt to changing conditions. Common techniques are multi-agent planning, dynamic programming, partially-observable Markov decision processes, constraint satisfaction, and distributed optimization algorithms [5].

**Decide & Act:** The **Decide** phase decides among candidate security plans based on observations of evolving security and privacy situations, with classification and filtering of the problems. The observations and their meanings from the **Observe** & **Orient** phases establish the input and derived knowledge for the Decide phase. Due to the complexity of decision making at this stage various trade-offs for optimal decision and information uncertainty should be done using appropriate models such as Bayesian networks, subjective logic, and fuzzy logic so as to accelerate the decision process and improve the degree of belief in sensory data. The **Act** phase initiates selected internal and/or external processes for either directly implementing countermeasures in the CPS-IoT devices or changing the physical CPS-IoT devices through the actuators at the Adaptive Data Collection and Automation layer.

### *C. Dynamic Security Knowledge Base*

A dynamic security knowledge base of vulnerabilities and threat intelligence will dynamically capture a range of information from its CPS-IoT environments. This information represents a context which is an important challenge in the complex networks and increasing ubiquity of the technologies deployed in the healthcare ecosystems.

Ontologies present the most promising instrument for context modelling and managing due to their high and formal expressiveness and the possibilities for applying ontology reasoning techniques. Utilizing these capabilities within ontologies can facilitate the dynamic capabilities. Dynamic vulnerability scanning and pentesting can also be applied to continuously test and monitor changes, diffs, new vulnerabilities and threats, non-assured security and privacy properties, etc. as evidence for the proper functioning of the cognitive-intelligence properties of the complex healthcare ecosystems.

### *D. Cross-Cutting Techniques*

*AI Techniques:* They are used for predictive analytics in the cognitive cycle model and combine cognitive methods (e.g., contextual and behavioural analysis, machine learning, and reasoning. Cognitive techniques have successfully been used for early detection of cybersecurity events [13].

*Run-time verification*: In [14], four run-time verification enablers are described and integrated into an adaptive control feedback loop: Models@run-time, Requirements@run-time, Dynamic Context Monitoring, and Runtime Verifier. Similarly, the Models@run-time enabler can be integrated into the Orient, Learn, Decide and Act phases, and Actuators of the architecture for the management of cybersecurity for critical healthcare infrastructures. The Requirements@run-time enabler can be integrated into the **Observe**, **Orient** and **Learn** phases of the control loop and Collectors of the architecture to support incremental verification the ability to trace changes to requirements. The Dynamic Context Monitoring can be integrated into the **Observe** phase and Collectors to monitor dynamic context (e.g., threat scenarios and even monitoring requirements) which is constantly changing at run-time and to adapt to context change. This thereby enables run-time verification with relevant monitoring mechanisms that keep track of aspects to validate. Finally, the run-time verification component (Runtime Verifier) can be integrated into the **Orient**, **Plan** and **Learn** phases to verify outputs from these phases enabling verification of an adaptation plan before or after instrumenting it.

*Evidence collection and tracing all the time:* dynamic evidence collection, tracing and mapping the evidence in order to analyse and identify the origin of the crime/incident all the time will enhance the degree of efficiency and reliability of capturing and tracing evidence dynamics. AI and deep learning techniques are helpful in dynamic forensic investigation. This offers robust intelligence and evidence during investigations and crime reconstructions, and helps to establish dynamic evidence based collection and evidence based risk management approaches.

### E. Adaptive Data Collection and Actuation

Adaptive data collection refers to the collection of security related data to improve collection efficiency, to ensure collection accuracy, to reduce the amount of collected data to minimize the effect of data collection, and to automate the data collection by adjusting to different environmental contexts and situations. Therefore, it is important to design of high-speed and scalable data collection platforms for real-time and historical security analytics [7]. To secure healthcare critical infrastructures and services security related data must be collected and analyzed in an intelligent, resilient, reliable, secure and timely manner fulfilling all the communication requirements and standards to detect attacks. Predictive/regression algorithms such as linear regression, Support Vector Regression (SVR), logistic regression, KNN regression will be investigated for the lightweight analysis of adaptive strategies. Deep learning mechanisms will be used for the identification of complex risk and attack patterns.

### F. Roadmap for Implementation

The different components of the proposed approach are being implemented in various research projects. Four modules, (i) adaptive intelligent monitoring and data collection of security related information, (ii) predictive analytics over the collected data based on AI-based (i.e. deep learning mechanisms), (iii) stakeholders' collaboration in vulnerability assessment, risk analysis, threat identification, threat mitigation, and compliance, and (iv) security knowledge base are being prototyped in [15]. These modules can be adopted and enhanced in our proposed approach for (a) adaptive data collection and actuation, (b) cross-cutting predictive analytics services, (c) privacy-aware collaboration, and (d) dynamic security knowledge base, respectively.

An initial study [2] has demonstrated the effectiveness of the development and integration of innovative and intelligent mechanisms for security, privacy, metrics and run-time verification. These can easily be adopted and enhanced in this approach for the innovative mechanisms. The methods for situational awareness and resilience to obfuscation to deal with adversarial activities in changing environments with special focus on the IoT forensics being developed in [16] can be adopted and enhanced for the cross-cutting dynamic forensics services. The adaptive data collection for real-time security analytics being developed in [17] can also be integrated in the adaptive data collection module of this proposed approach. Finally the framework for simulating the human cognitive behaviour will be developed.

## V. Conclusions and future work

This paper presents the conceptualization and description of a cognitive cybersecurity architecture for simulating the human cognitive behaviour to anticipate and respond to new and emerging cybersecurity and privacy threats to CPS-IoT enabled healthcare ecosystems. To achieve this, it combines artificial intelligence, cognitive methods, forensics, and innovative security mechanisms as cross-cutting services. It is structured in four layers, collaborative, perception and knowledge, data collection and actuation, and infrastructure. This architecture is developed based on different concepts developed in different projects the author is participating.

In our future work, we plan to focus on defining details of the different components of the architecture and validate them through a set of simulations and demonstration systems in real or realistic use scenarios. We also plan to address the human side cognitive perspective such as cognitive overloads and biases.

## Acknowledgment

The work presented here has been carried out in three research projects: The IoTSec (Security in IoT for Smart Grids, Nr. 248113/O70) and ArsForensica (Computational Forensics for Large-scale Fraud Detection, Crime Investigation and Prevention, Nr. 248094/O70) projects funded by the Research Council of Norway, and FINSEC (Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures) project funded by the EU under the Horizon 2020 programme (contract number: 786727)

## References

[1] H. J. Wilson, The Cognitive Usefulness of the Internet of Things, Harvard Business Review, Nov. 17, 2014

[2] H. Abie and I. Balasingham, Risk-Based Adaptive Security for Smart IoT in eHealth. In BODYNETS 2012, 2012, 269-275

[3] D. Miessler, HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack, HP Fortify, July 29, 2014

[4] Lynne Coventry and Dawn Branley-Bell. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 113. 10.1016/j.maturitas.2018.04.008.

[5] Karen Zita Haigh and Craig Partridge. 2011. Can artificial intelligence meet the cognitive networking challenge? Dayton, OH. http://www.cs.cmu.edu/~khaigh/2011-haigh-EURASIP-JWCN.pdf

[6] W.J. Chisum and B.E. Turvey, Evidence dynamics: Locard's exchange principle & crime reconstruction. Journal of Behavioral Profiling 1(1) (2000)

[7] Cognitive Cybersecurity Intelligence (CCSI) Group, IBM Research, https://researcher.watson.ibm.com/researcher/view_group.php?id=4354, accessed 27.01.2019

[8] Margaret Rouse, cognitive security, https://whatis.techtarget.com/definition/cognitive-security

[9] V. Lenders, A. Tanner, A. Blarer, Gaining an Edge in Cyberspace with Advanced Situational Awareness, IEEE Security & Privacy Vol.:13 (2), 65-74, 2015

[10] A. Yelizarov and D. Gamayunov, Adaptive Visualization Interface That Manages User's Cognitive Load Based on Interaction Characteristics. In Proc. of VINCI, Tony Huang (Ed.). ACM, New York, USA, 2014, 1-8.

[11] J. Cho et al., Stram: Measuring the trustworthiness of computer-based systems. to appear in ACM Computing Survey, 2019.

[12] Ullah, F., and Babar, M.A (2018) 'Architectural Tactics for Big Data Cybersecurity Analytic Systems: A Review', Arxiv.Org. 1–48 (2018)

[13] Sandeep Narayanan et al., Cognitive Techniques for Early Detection of Cybersecurity Events, arXiv:1808.00116v1 [cs.CR] 1 Aug 2018

[14] Arild B. Torjusen, Habtamu Abie, Ebenezer Paintsil, Denis Trcek, and Åsmund Skomedal. 2014. Towards Run-Time Verification of Adaptive Security for IoT in eHealth. In *Proceedings of* ECSAW '14. ACM, New York, NY, USA, Article 4, 8 pages.

[15] FINSEC (Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures) project, https://www.finsec-project.eu

[16] Ars Forensica (Computational Forensics for Large-scale Fraud Detection, Crime Investigation & Prevention) project, https://www.ntnu.edu/iik/digital_forensics/ars-forensica-rcn-project

[17] IoTSec (Security in IoT for Smart Grids) project, http://iotsec.no/

[18] J. Cho et al., Stram: Measuring the trustworthiness of computer-based systems. ACM Computing Survey (under review), 2019.