

# Cyber-Physical Systems and Humane Security Engineering

Gopal T. V.

Professor, Department of Computer Science and Engineering, College of Engineering, Anna University, Chennai  
Tamil Nadu, India.

Email: [gopal.tadepalii@gmail.com](mailto:gopal.tadepalii@gmail.com); [gopal@annauniv.edu](mailto:gopal@annauniv.edu)

**Abstract:** There is plenty of on-going research in the area of supporting protocol stacks, crypt systems and formal methods. Multicast authentication is a critical security service in mobile and sensor networks. Cyber-Physical Systems [CPS] are controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. The interaction patterns are increasingly becoming complicated. Unless, humane approaches are introduced in security engineering the computer-based approaches become increasingly sophisticated, faster, expensive and complex. These solutions are replete with several vulnerabilities leaving ample scope for breaches resulting in serious tangible and intangible losses to the organizational assets. This paper has a focus on the human integration in CPS. It also positions the analog systems in the digital space. Humane Security Engineering is intended to result in civilizing effect on people.

**Keywords:** Algorithms, Cyber-physical systems, Humane security engineering.

## I. INTRODUCTION

The explosion of mobile devices, server virtualization, Bring Your Own Device [BYOD], Internet of Things [IoT] and Content are among the most important technology trends that make the modeling of networking architectures as Cyber-Physical Systems [CPS] an imperative need. The complex relationships governing the behavior of software for CPS can anticipate vulnerabilities and risks across multiple infrastructure systems.

Organizations [1] have rapidly increasing opportunities to tap into a virtual, on-demand workforce. However, the challenges of this latest wave require several new management models and skills. Cyber-Physical Systems [CPS] are interacting networks of physical and computational components. The term physical in this context refers to the space governed by the Laws of Physics. Modern automobiles, smart buildings, wireless implants, intelligent traffic lights, full-body scanners, and industrial control systems are realistic examples in the physical space. CPS use wireless technologies, sensing and distributed

decisions based on ubiquitous computing and networks with potential benefits in very diverse areas of human endeavor. Several emerging concepts such as subjects and objects with associated practices spanning across technology centred and complementary automation strategies are resulting in many challenging contexts in the CPS. It is becoming increasingly clear that the state-of-the-art practices are inadequate in many cases in the context of CPS.

A cyber-physical attack [1] is a security breach in cyberspace that adversely affects physical space. In the recent past there have been several incidents in vital domains such as Energy, Water, Health, Transportation and Defense. CPS deeply integrate computation, communication, and control into the physical systems. Software has been the adhesive for many of these multidisciplinary CPS. The core engineering disciplines have been banking on the well formulated design principles unlike Software. CPS breaches imply the misuse of a cyber process to affect a physical one. They have an impact in both cyberspace and physical space.

Armed conflicts, terrorism, organized crime, pandemics, and natural or man-made disasters are the major causes of insecurity among the citizens. Security is a perception to begin with. Humane security engineering mitigates any multiplier effects in the perception of threats and vulnerabilities and the method is assuring for a given individual.

CPS security [2] is an outcome of Physical, Political, Socio-Economic, Cultural, Environmental and Information. Privacy is concerned with the collection and use of personal data. Security is concerned with protection of that personal data from unwanted intruders. "Privacy" and "Security" are inter-related. However, Privacy is personal. It can be governed by "informed consent" across the stakeholders. Privacy concerns include the physical body, behavioral traits and characteristics, communications, data, image, thoughts, feelings, location, space and association with other beings. Security is impersonal. It is like a fence around a field.

Technology is readily available and affordable. It comes along with an enormous unmeasured value provided by the free entertainment, free services and information available through the extensive use of Information and Communication

Technologies [ICT]. The technologies introduced in the late nineteenth century resulted in three generations of relatively high productivity growth. It is useful to observe that with ICT, the pace of economic and social transformation has slowed in recent decades, not accelerated. Security in CPS needs to factor the pronounced instability in countries around the world caused by the current global economic crisis.

Education and Training of the Human capital is as important as the traditional investments in hardware and equipment. Globalization warrants understanding of foreign countries and cultures and to speak certain foreign languages. Education is not a magic wand. Humane Security Engineering thrives *on meaningful information and tools for creating a safe and humane world.*

The most dominant shift in computational techniques and technologies is the unprecedented growth in the number of smart edge devices [such as smart phones, tablets, smart watches, smart glasses, smart meters, connected vehicles and so on] being used by virtually every individual. These smart edge devices double up to offer a massive infrastructure for computing. Individuals are sharing their homes, cars, and even meals when they are rewarded for it. It is reasonable, to infer that the owners of the devices share their data and infrastructure in return for a reward. The dominant communications technologies are wireless and mobile communications.

Human interaction [3,4] with CPS begins with “user authentication” that involves personal data. Eighty-five percent of customers are dissatisfied with current authentication methods. Often times, it results in risky password reuse, password amnesia and high abandonment rates. Eventually, enterprises lose revenue and get exposed to high security risks in the CPS. Businesses have taken to an omnichannel approach, seamlessly integrating every channel to deliver the ideal brand experience to customers and the other stakeholders. A comprehensive User Identification and Authentication layer comprising services such as secure Single Sign-On (SSO), scalable access and centralized control, and a unified view of the user, can be easily added to existing CPS, dramatically improving the user experience and security.

Security Engineering in CPS is an effective deployment of one or more of the following strategies.

1. What the User and User Only Knows [Example: Password]
2. What the User and User Only Has [Example: Hardware Key]
3. What the User and User Only Is [Example: Bio-Metrics]

The research reported in this paper has the primary objective of simplification of the increasingly complex computational methods by integrating the humane aspects in security engineering. It is about building systems to remain dependable

in the face of malice, error, or mischance. The term “human user” extends the notions of individuals and their cognitions to include the tasks and interactions with various groups of people, organizations, and communities at large. Most of the existing crypt systems are truly beyond the ken of a typical individual resulting in the need for super specialists in this area to provide high dependability of the systems and assure high Quality-of-Life. Many devices and systems based on high-end cryptographic techniques are now quite pervasive across human communities. Humane Security Engineering is to design our protocols and methods around the limitations of these expensive and difficult to comprehend systems. This paper proposes a shift of focus from compute intensive highly advanced crypt systems to people and community based participatory methods.

Humane Security Engineering in the context of CPS warrants:

- Comprehensive understanding of the complete spectrum of types of human-in-the loop considerations.
- Extensions to system identification or other techniques to derive models of human behaviors including intentionality and free-will.
- Incorporation of human behavior models into the formal methodology of evolving complex systems.

Presently, security is a multi-disciplinary challenge. It is a strategy that has to be built into every facet of the business. The various job roles in the domain human-machine systems have been well delineated. Function allocation based on a set of specific technological capabilities and mathematical modeling tools was the first step. Advances in computing techniques and technology using sensors and actuators extend the functional capabilities to factor perception and cognition. The quest is truly for systems that accommodate a broad range of skills and stimulate the development of skills within the framework of CPS. There is a balance needed between security and privacy. Citizens, organizations, and other communities accept a certain level of intrusion, provided a certain level of security is afforded. Also, every individual, organization, and community, has a different level of sensitivity to intrusion and a different notion of acceptable security risk.

## II. SAMPLE APPLICATIONS - AUTOMOBILES AND PLACES OF SPIRITUAL WORSHIP

The impetus for security breaches in the CPS is not only the lack of material well-being but also the denial of opportunities. Social Exclusion due to lack of resources to participate or exclusion because of ethnicity, disability, gender and so on can result in security breaches. In other words, the unequal distribution of social and societal advantage is the underlying force that creates conditions for security breaches.

This section illustrates the aspects mentioned above with two simplified applications. Places of Worship are seldom studied formally from the perspectives of Security Engineering in Cyber-Physical Systems. Both automobiles and places of worship that are so common in a social system make the design, development and management of computer-based systems highly expensive and not so cost-effective in assuring adequate security. Both these applications exhibit large coupling factor making the designs for any security highly vulnerable.

#### A. Automobiles

The automobile has been developed based on the laws of mechanics and the chemical equations. Today it is equipped with many electronic components and control systems to improve performance and safety. The astounding growth in Human Mobility warrants a strong coupling between the physical movements of people at various scales and the technology centered automation strategies. The proportion of local and global Information that needs to be processed in the current automobile is a major challenge. The door-locks, radios, sensors and all the other technology has evolved rapidly. A set of plug-in interfaces enable a mobile phone to handle communications, human-driven navigation and entertainment [5]. Thought-controlled cars and cars for the differently - abled are on the anvil. User authentication checks are now imperative. As a matter of fact, the mobile phone of the user can authenticate itself to the vehicle, and take over the console display.

Connected Vehicles offer better access to the internet, and an anti-crash system allows for car-to-car data-sharing protocols. This is in addition to the existing network of sensors already embedded in roads and highways. There are more challenges in consumer demands, technology development, globalization, integration and collaboration. Self-driving cars that manoeuvre around traffic jams and interact with other things on the Internet including smart homes are emerging. There is plenty of on-board diagnostics as well. It is expected that over the next few years, continued evolution in sensors, computing power, machine learning, and big-data analytics will bring us closer to the goals of zero accidents and real-time traffic management. It is estimated that a typical automobile will soon require 200 million to 300 million lines of software code.

Analytics to extract information from pictures, from video, and from laser ranger data and recognizing the patterns within such information remain as core challenges. Many methods to prepare features from a range of signals and then detect the source of the signal are emerging. CPS to identify the scenario (for example: a city, forest, or race course) or estimate the free space and anticipate the major physical obstacles are proving to be very challenging to design and develop. Since, many vehicular users are expected to request the same common data such as weather and environment information over a given area multicasting is often needed.

#### B. Places of Spiritual Worship

Many places of spiritual worship have associated institutions to provide services to disadvantaged groups through outreach programs. These can include charitable services to individuals and groups such as the homeless, mentally ill, victims of crime or natural disasters, reformed criminals, substance abusers, and many other types of people [6]. Many people who have had difficulties seek help from local spiritual institutions.

The core characteristics of the places of spiritual worship in the service of people voluntarily subscribing to the corresponding faith are:

- Contact with the public through regular prayer and other similar meetings.
- Exchange of money in the form of donations and other charges related to types of worship.
- Working with unstable persons seeking comfort.
- Working with people seeking solitude or in small groups.
- Working at night or late hours.
- Working in a high-crime areas.
- Working in community-based contexts that act on faith and beliefs rather than logic and reason.

Accessing and using technology has now become the norm for places of worship. The scholars associated with the places of worship are seeking to reach more people in more places, while at the same time providing a compelling spiritual experience. Point-to-Point, Point-to-Multipoint, and Multicast Video over IP networks for live and file-based video playing and distribution are now affordable and widely used for this purpose.

CPS including the places of spiritual worship are challenged by severe aggression and/or behavior issues, chemical dependency and abuse, sporadic violence and other obnoxious social tendencies. Some of the behavior characteristics of associated people to facilitate humane security engineering for such places of spiritual worship are given below.

- Coping with conflicts, disappointments, failures, insults, or other stresses encountered in everyday life.
- Expressing anger or rage, frustration, disappointment, humiliation, sadness, or similar feelings.
- Demonstrating or failing to demonstrate resiliency after a setback, a failure, real or perceived criticism, disappointment, or other negative experiences.
- Self-esteem and self-perception - how the individual feels about himself/herself.
- Respond to rules, instruction, or authority figures.

- Demonstrating or expressing a desire or need for control, attention, respect, admiration, confrontation, or other needs.
- Demonstrating or failing to demonstrate empathy with the feelings and experiences of others.
- Internalizing or externalizing blame.
- Perception of others around and necessary etiquette of interaction with them.

The proposed methods make security perception intuitive and hence readily managed within a given community rather than a highly skilled expert with expensive machinery.

### III. CHALLENGES IN MOBILE / SENSOR NETWORK BASED AUTHENTICATION IN CPS

CPS operates with inherent uncertainty, context dependencies and adversarial certainty arising from both the cyber and physical worlds. Provenance which refers to the source of the data / service is the first challenge in CPS. The source ought to be secure and traceable, and that the data / service is delivered without unauthorized modification. Social engineering, emerging security standards, vendor control, access control implementation and authentication are well known strategies for designing CPS.

Security of these CPS depends on integrating a wide variety of sensors and controllers / actuators. Most of these devices interacting with the physical world are extremely fragile to security breaches. Bring Your Own Device [BYOD] is very attractive but they tend to be insecure-by-design implementations and often times software updates to patch vulnerabilities are next to impossible. End-Point Security refers to a methodology of protecting the corporate network at the potential entry point for a remote device. There are several commercial suites in the market to provide End-Point Security. The challenge has been to balance threat prevention and detection. Threat analysis and automatic containment is the core strategy in End-Point Security suites.

Trustworthiness of the devices may be improved by Attestation [7]. Attestation allows unauthorized changes to a device to be detected. One of the trust establishment mechanisms allows a platform (the attester) to reliably vouch on its current state to a remote verifier (the challenger). This mechanism allows the challenger to obtain confidence in the trustworthiness of the attester through hardware-based security mechanisms.

Trusted Platform Module is at the core of this method and it usually demands additional dedicated hardware. This may be expensive and not feasible at times. Structural type of attestation presupposes the CPS within which trust exists. Software attestation enables a verifier to check the integrity of the memory contents of another device (the prover) against

modifications by malicious code. Interpersonal type of software attestation is agent & context specific. Dispositional type is not. There are many more challenges in authentication.

In the mobile communication systems, the radio waveform is easily eavesdropped. Many sensors in the CPS are unattended resulting in vulnerabilities due to limited energy and computing power. The inherent heterogeneity in the CPS and latency due to the horizontal and vertical [upward / downward] handoffs usually result in lossy protocol conversions and transmissions. CPS is very vulnerable to the following breaches.

- Physical Attacks: Manipulating the devices and malicious code.
- Compromise of Credentials: Broken authentication mechanisms.
- Configuration Attacks: Fraudulent software update / configuration changes.
- Protocol Attacks on the Device: DDoS, Over-the-Air Management breaches.
- Attacks on the Core Network: Breaches in the backbone.
- User data and identity privacy attacks / breaches.
- Fraudulent disclosure of confidential data.
- Integrity loss due to malicious modification of sensory data and commands to the actuators.

There is plenty of research based on designing; verifying and validating advanced networking protocols to address the above challenges. However, these efforts have been technology-centric. Modeling the security threats in CPS based on systems theoretic approaches are enabling improved verification of the protocols. However, presently this approach is limited in scope and the results are case based.

### IV. SECURE DESIGNS FOR PEOPLE

CPS is a driver of many innovations in the context of multi-disciplinary services and solutions. Designing and developing CPS for people warrants very advanced solutions for complexity stemming from data heterogeneity, reliability, data management, privacy, security and real-time performance [3,4].

Multicasting [8] is an efficient method of communication to deliver services from a given server / source to a large group of users. This technique provides proficient and best-effort delivery service. The service providers must ensure that authorized users alone access the service. This is usually done by using an access control mechanism, which authenticates the users or ensures that only the authentic users access the service. It is imperative to establish the source for the data / service through strategies outlined in Section 3 of this paper. User authentication implies transmission of multimedia data such as audio, video, image

and text about the user and the context of usage. Protocols have been developed for user ‘join and leave’ requests [9,10]. There are several associated crypt systems and current user tree maintenance algorithms being developed by several research groups worldwide.

There are several methods for comparing the cost of delivering multimedia data through multicast traffic, and the effects of bandwidth, latency, jitters, loss of packets, and efficiency on transmission. These are the typical Quality-of-Service [QoS] metrics. Authentication is thus becoming more challenging and expensive in CPS due to the sophistication warranted to improve the QoS. This in turn results in a manifold increase in

the costs passed on to the users.

Further to these algorithmic strategies that are technology-centric, the author proposes the multimedia data analytics using the block schematic depicted in Fig. 1 [11]. These analytics are related to Quality-of-Experience that encompasses all user related aspects. This in addition to the Quality-of-Service based metrics of the seven - layer ISO - OSI Reference Model. This paper has a focus on the analytics related to User Collocation and Symmetry.

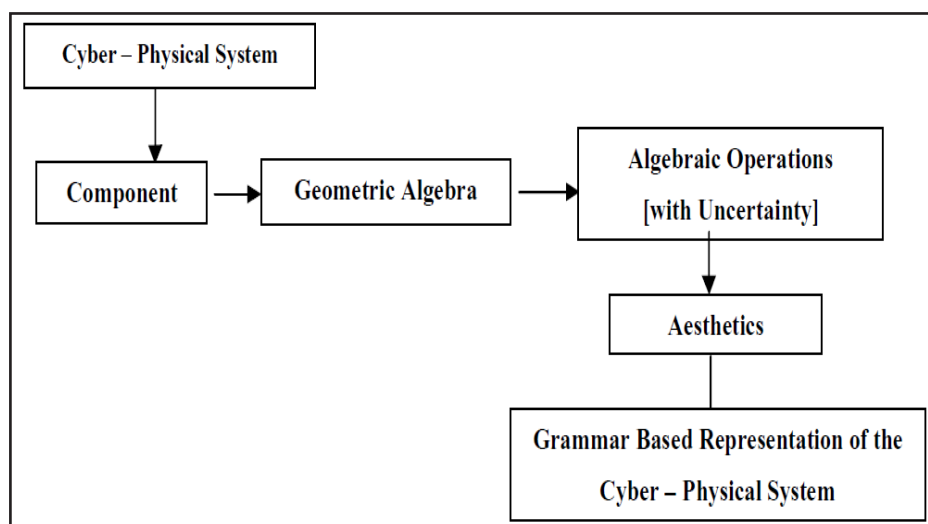


Fig. 1: Block - Schematic for Multimedia Data Analytics in CPS

The aesthetic attributes [11] are given in Fig. 2.

Form	Surface	Motion	Sound	Text
Position	Color	Direction	Tone	Label
Size	Texture	Speed	Volume	
Shape	Blur	Acceleration	Rhythm	
Rotation	Transparency		Voice	
Resolution				

Fig. 2: The Aesthetic Attributes

Geometry is always in tandem with other topics of mathematics such as algebra, arithmetic, mathematical analysis and the theory of functions. The theodolite, the compass and the pantograph are some of the instruments that are used to create the precision necessary for the measurement of the objects. Geometric Algebra [GA] is a powerful mathematical language for expressing physical ideas. Geometric Algebra promises to be a unifying language for physics and mathematics [12].

GA has been used to work with Maxwell’s Equations, Gibb’s Vectors, Computer Vision, Computer Games, Black Holes, Cosmology and related domains of comparable complexity. The CPS using GA is considerably complex and useful in their Computational Analysis.

Aesthetics form an *attracting set* for a dynamical system as a closed subset *A* of its phase space such that for “many” choices

of initial point the system will evolve towards  $A$ . *Attractor* is an attracting set which satisfies some supplementary condition, so that it cannot be split into smaller pieces. Attractors can take on many other geometric shapes [phase space subsets] But when these sets [or the motions within them] cannot be easily described as simple combinations (e.g. intersection and union) of fundamental geometric objects [e.g. lines, surfaces, spheres, toroids, manifolds], then the attractor is called a strange attractor [13]. In the simplified applications presented in Section 2 of this paper, the Car of a Very Very Important Person [VVIP] is an attractor and likewise a well known place of worship is an attractor. These models are also useful in impacting the cognitive capabilities of the authenticated users for improved Security Engineering.

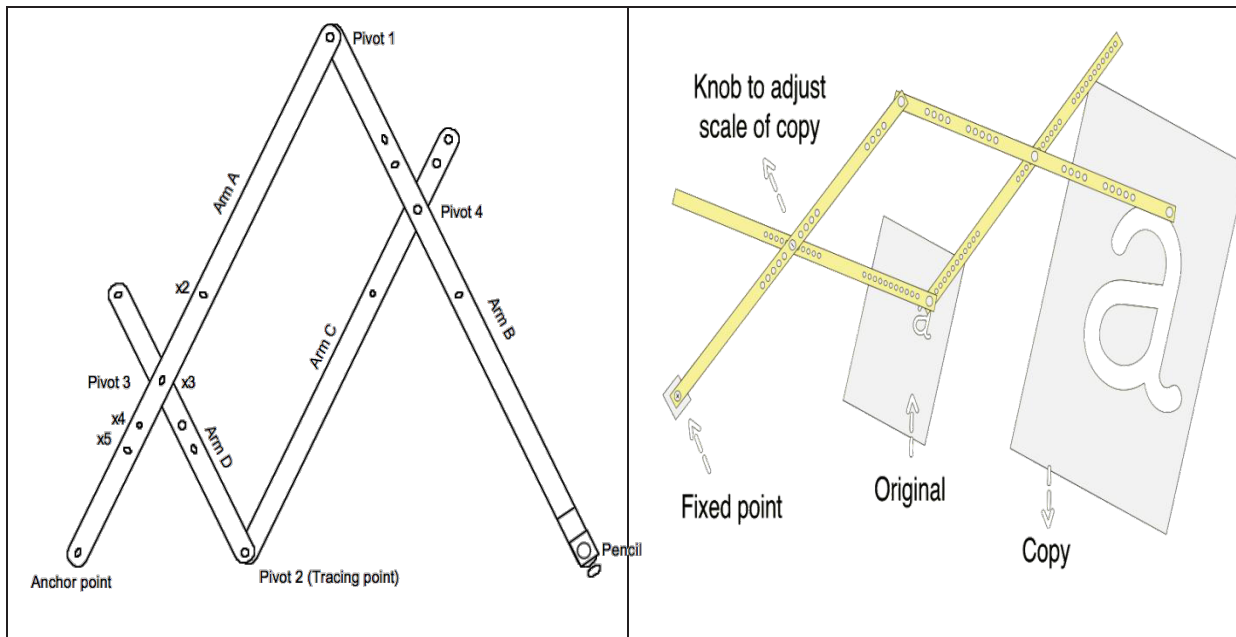


Fig. 3: Pantograph and its Working

For the present purpose, the generalized Pantograph equations with variable co-efficients [14] given below are used.

$$u^{(n)} = \sum_{j=1}^J \sum_{k=0}^{n-1} P_{j,k}(x) u^{(k)}(\alpha_j x) + f(x), x \in [0, T]$$

with the initial conditions as:

$$u^{(k)}(0) = a_k, k = 0, 1, \dots, n-1.$$

The proposed method is not to introduce another variety of perceptions based on the scaling factor due to the Pantograph. The equations given are indicate formal verification if necessary.

The boundary value problems when the conditions are given at both endpoints of  $[0, T]$  are also considered. There are many approaches to solving these equations reported in the learned journals [15, 16].

To quickly create relatively cheap terrain models for a broad public, a mechanised production technique was used in

## V. DETECTING AUTHENTIC USER COLLOCATION AND SYMMETRY

This paper has the focus on security engineering in CPS with respect to Authentic User Collocation and Symmetry. The authentication strategies are proposed in the previous sections of the paper. Geometric algebra directly computes with subspaces thus simplifying many geometrical operations. This paper proposes for the first time Pantograph based Humane Security Engineering. A Pantograph is an instrument for copying a plan or drawing on a different scale by a system of hinged and jointed rods. The pantograph and the way it works are depicted in Fig. 3.

Germany, Italy, France and the USA. This historical technique uses a pantograph to guide a milling cutter. *Pantograph* is used as an apparatus mounted on the roof of an electric train, tram or electric bus to collect power through contact with an overhead *catenary* wire. There are very well-known applications of systems using Pantograph.

Pantograph is a dynamical system whose behavior is specified over any given short period of time. To determine the system's behavior for a longer period, it is often necessary to integrate either through analytical means or through iteration. The "phase space" represents all possible states with each possible state corresponding to one unique point in the phase space. The subset of the "phase space" of the dynamical system corresponding to the typical behavior is the attractor specified as Aesthetics.

As people visit various places in their daily lives, connections are formed amongst people either based on the place or on the other people. Collocation methods for modeling the social and

geographical context based on collocation networks in human mobility datasets improve the humane element in Security Engineering.

A collocation method [17,18] chooses a finite-dimensional space of candidate and a number of points in the domain [called *collocation points*], and to select that solution which satisfies the given equation at the collocation points. All these collocation methods are in fact implicit Runge-Kutta methods. However, numerical computation is iterative and the necessary approximations may result in large errors in the behavior of evolving complex CPS. The author suggests an analytical method using geometric algebra first to quickly understand the mechanism and physical effects through the model. The idea is to build a geometry model rather than develop an iterative approximation of the geometry [19] and directly use it in analysis. Nudging digital after this is a Viable System Model.

Symmetry [20,21] is pervasive in both natural and man-made environments. Humans have an innate ability to perceive and take advantage of symmetry in everyday life. Geometry proves to be better in automating this powerful insight. Virtually every field of analysis including CPS can be simplified by identifying the innate symmetries at the earliest. There are many aspects of logical structure in computation that involve the study of symmetry in some form. Fig. 4 reflects the potential of the insight accorded by symmetry that is not obvious in the numerical computation.

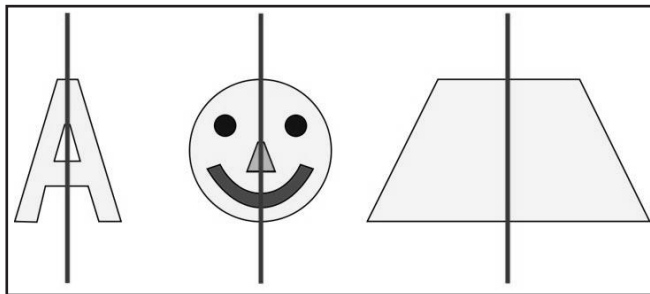


Fig. 4: Symmetry

Hands and feet, paces and faces, polygons and legs are among the many body references used in measurement and geometry to this day [22]. By involving human bodies in mathematical reasoning, we can better understand geometric concepts and facilitate developing spatial sense by using what Seymour Papert called “body-syntonic reasoning” [23]. The assumption is that the human being involves with the activity on hand resulting in a trace to the human being after authentication.

Advanced Computer Graphics, Workstations with Large Monitors and Graphics Processing Units [GPU] Programming make Geometry a very attractive initial method for authentication related processing. Collocation and Clustering for Automobiles and Places of Spiritual Worship are modeled using Attractors. Pantograph can have points as mirror reflections representing

symmetry and can also half a complex number. Using these properties of the Pantograph equation Collocation and Symmetry of Authentication requests are projected on to an imaginary plane [24]. In other words, the original “Collocation and Symmetry” detected in the authentication requests are projected to a scale based on the historicity of their occurrence. If the scale is high a Humane Security Engineering vulnerability or threat is triggered. A *pantograph* is a dynamical system amenable for risk, reliability, safety analysis and complex failure mode analysis.

This novel method being experimented with in Computational approaches in Cyber-Physical Systems that are complex and evolving.

## VI. CONCLUSIONS

The core characteristics of CPS include:

- Small inputs can lead to dramatically large consequences.
- Very slight differences in initial conditions produce very different outcomes.
- Global properties flow from aggregate behavior of individuals.

Ordinary Differential Equations [ODEs] have been used to model physical phenomena since the concept of differentiation was first developed. The various parameters used by the Interval Manager [IM] result in delayed effects in a differential equation resulting in Delay Differential Equation [DDE]. Job arrival patterns for the schedulers in Operating Systems were the very early formalisms. Hidden Markov Models have also been used by systems designers. This paper proposes a new approach to Humane Security Engineering.

User Authentication, Collocation and Symmetrization methods reported in this paper are more efficient using Geometry rather than the DDE. Geometry is more natural and aligns well with the humane security engineering methods. Many applications including digital video forensics [25] and special animation effects in movies benefit from the approaches reported in the paper.

Security is a matter of perception. All over the world, only a select few deal with these perceptions resulting in overt centralization of the core concerns and war like conditions. The paper is to model the world view of a typical citizen who is capable of helping the de-escalation of several concerns and perceptions.

In conclusion, the reported research in this paper works around the limitations of the existing increasingly expensive and complex computer-based solutions to integrate the human in the loop for simplification.

## REFERENCES

- [1] G. Loukas, *Cyber-Physical Attacks - A Growing Invisible Threat*, Elsevier, USA, 2015.
- [2] C. Marti, "A survey of the European security market," *Economics of Security Working Paper 43*, Berlin: Economics of Security, 2011.
- [3] B. Hadorn, M. Courant, and B. Hirsbrunner, "Towards human-centered cyber-physical systems: A modeling approach," *Technical Report*, January 2016.
- [4] R. Kling, and S. L. Star, "Human centered systems in the perspective of organizational and social informatics," *SIGCAS Computers and Society*, vol. 28, no. 1, pp. 22-29, March 1998.
- [5] S. Shibu, and S. Jain, "Pervasive computing for automobiles: An approach to maximize user convenience and safety using VANETs," *International Journal of Computer and Electrical Engineering*, vol. 2, no. 6, pp. 1053-1058, December 2010.
- [6] J.-L. McLamb, *Keeping Religious Institutions Secure*, Elsevier, USA, 2015.
- [7] J. Valente, C. Barreto, and A. A. Cardenas, "Cyber-physical systems attestation," *2014 IEEE International Conference on Distributed Computing in Sensor Systems*, Marina Del Rey, California, USA, pp. 354-357, 2014.
- [8] T. V. Gopal, "Engineering software behavior in cyber-physical systems," *International Journal of Engineering Issues*, vol. 2016, no. 1, pp. 44-52, 2015.
- [9] R. Pugalenth, and T. V. Gopal, "Performance evaluation of multimedia data in heterogeneous network using multicasting with kerberos protocol," *International Journal of Soft Computing*, vol. 8, no. 4, pp. 247-251, 2013.
- [10] R. Pugalenth, and T. V. Gopal, "An efficient and variable interval rekeying for dynamic Ad Hoc multicast groups using key path reduction," *Journal of Computer Science*, vol. 10, no. 8, pp. 1281-1290, 2014.
- [11] T. V. Gopal, "The physics of evolving complex software systems," *International Journal of Engineering Issues*, vol. 2015, no. 1, pp. 33-39, 2015.
- [12] J. Lasenby, A. N. Lasenby, and C. J. L. Doran, "A unified mathematical language for physics and engineering in the 21<sup>st</sup> century," *Philosophical Transactions of Royal Society of London, A*, vol. 358, no. 1765, pp. 21-39, 2000.
- [13] V. P. Kruglov, S. P. Kuznetsov, and A. Pikovsky, "Attractor of smale - Williams type in an autonomous distributed system," *Regular and Chaotic Dynamics*, vol. 19, no. 4, pp. 483-494, 2014.
- [14] M. Sezera, and A. Akyuz-Dascioglu, "A Taylor method for numerical solution of generalized pantograph equations with linear functional argument," *Journal of Computational and Applied Mathematics*, vol. 200, no. 1, pp. 217-225, 2007.
- [15] G. Makay, and J. Terjeki, "On the asymptotic behavior of the pantograph equations," *Electronic Journal of Qualitative Theory of Differential Equations [EJQTDE]*, no. 2, pp. 1-12, 1998.
- [16] M. M. Bahsi, and M. Çevik, "Numerical solution of pantograph-type delay differential equations using perturbation-iteration algorithms," *Journal of Applied Mathematics*, vol. 2015, pp. 1-10, 2015.
- [17] S. Yu. Reutskiy, "A new collocation method for approximate solution of the pantograph functional differential equations with proportional delay," *Applied Mathematics and Computation*, vol. 266, pp. 642-655, 2015.
- [18] W. Ming, and C. Huang, "Collocation methods for Volterra functional integral equations with non-vanishing delays," *Applied Mathematics and Computation*, vol. 296, pp. 198-214, 2017.
- [19] F. Auricchio, L. B. D. Veiga, T. J. R. Hughes, A. Reali, and G. Sangalli, "Isogeometric collocation methods," *Mathematical Models and Methods in Applied Sciences*, vol. 20, no. 11, pp. 2075-2107, 2010.
- [20] A. Guessab, and F. Guessab, "Symmetrization, convexity and applications," *Applied Mathematics and Computation*, vol. 240, pp. 149-160, 2014.
- [21] A. Guessab, "Symmetrization procedures and convexity in centrally symmetric polytopes," *Applied Mathematics and Computation*, vol. 243, pp. 74-82, 2014.
- [22] N. Naylor, *Naked Geometry*, Lulu, Inc., Raleigh, 2005.
- [23] S. Papert, *The Children's Machine: Rethinking School in the Age of the Computer*, Basic Books, New York, 1992.
- [24] G. Derfel, and A. Iserles, "The pantograph equation in the complex plane," *Journal of Mathematical Analysis and Applications*, vol. 213, no. 1, pp. 117-132, 1997.
- [25] A. K. Nayak, *Digital Forensics*, CSI Communications, Computer Society of India, Mumbai, vol. 39, no. 12, March 2016.