Cognitive Identity Management: Risks, Trust and Decisions using Heterogeneous Sources

S.N. Yanushkevich[1], W.G. Howells[3], K.A. Crockett[2], J. O'Shea[2], H.C.R. Oliveira[1], R.M. Guest[3], V.P. Shmerko[1]
[1]*Biometric Technologies Laboratory, Department of Electrical and Computer Engineering, University of Calgary, Canada,*
Web: http://www.ucalgary.ca/btlab, E-mail: syanshk@ucalgary.ca; helder@schulich.ucalgary.ca; vshmerko@ucalgary.ca
[2]*Department of Computing and Mathematics, Manchester Metropolitan University, U.K.,*
E-mail: K.Crockett@mmu.ac.uk; J.D.Oshea@mmu.ac.uk
[3]*School of Engineering and Digital Arts, University of Kent, U.K.,* E-mail: W.G.J.Howells@kent.ac.uk, R.M.Guest@kent.ac.uk

***Abstract*—This work advocates for cognitive biometric-enabled systems that integrate identity management, risk assessment and trust assessment. The cognitive identity management process is viewed as a multi-state dynamical system, and probabilistic reasoning is used for modeling of this process. This paper describes an approach to design a platform for risk and trust modeling and evaluation in the cognitive identity management built upon processing heterogeneous data including biometrics, other sensory data and digital ID. The core of an approach is the perception-action cycle of each system state. Inference engine is a causal network that uses various uncertainty metrics and reasoning mechanisms including Dempster-Shafer and Dezert-Smarandache beliefs.**

I. Introduction and Motivation

The future generation security checkpoint for mass-transit hubs and large public events is anticipated to be a system that combines: biometric-enabled authentication [12], [19], [31], [45] and watchlist check [32], screening strategies [37], deception feature detection [1], [41], [43], [55], as well as concealed illicit item detection [38], [53]. Such a system will be an integral part of the security infrastructure, including logistics and surveillance network with abilities of tracking individuals-of-interest and analyzing the group behavior. This vision is introduced, in particular, in the International Air Transport Association technology roadmap "Checkpoint of the future" [27].

The currently being developed concept of a future checkpoint is called a **cognitive checkpoint**. This concept is more complicated compared to the classic security paradigms such as layered security model [9], [29], [49], [54], or a dynamic individual risk update [37]. The cognitive checkpoint is a semi-automated system, which deploys the AI to process the data sources and to assess trust and risk; this assessment is submitted to a human operator for the final decision. Fig. 1 depicts the concept of cognitive identity management:

1) An individual is a subject of authentication and risk assessment based on acquired physical and virtual (online) sources of information. Four physical sources include data captured in the following bands:

- Source A: Acoustic domain as a human-machine communication channel with frequency range of 70 to 200 Hz for men, 150 to 400 Hz for women, and 200 to 600 Hz for children; the pitch, loudness and timbre of a human voice are the main parameters used by an e-interviewer for emotions and deception detection [1], [41], [55] [62];
- Source B: Infrared domain; the human body radiates non-visible infrared light ($3-12\mu m$ waves) in proportion to its temperature; this band is used for assessment of both cognitive and physical state [43];
- Source C: Visual domain, $400-700\mu m$, for authentication and emotional state assessment using face and face expression recognition [31], [32];
- Source D: Radar illumination, 3–10 GHz; certain concealed items can be detected using the Ultra Wide Band (UWB) radar [24], [38].

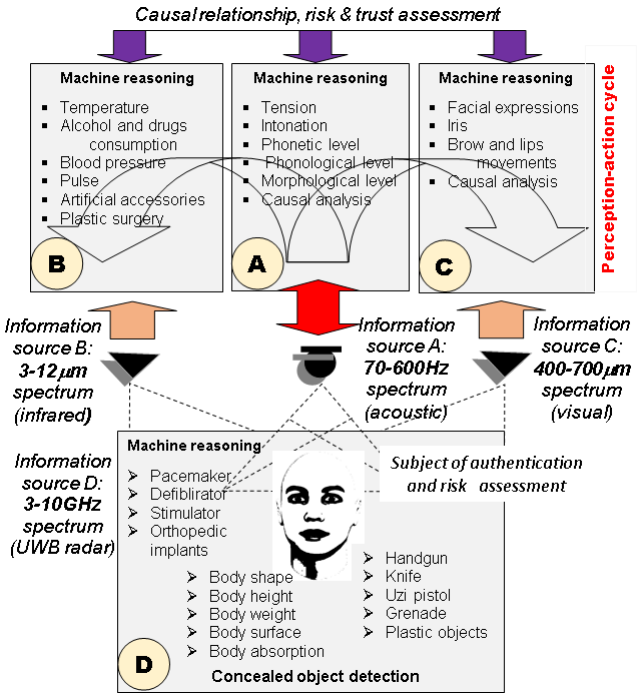


Fig. 1. Four information sources for machine reasoning at the security checkpoint: biometrics in infrared ($3-12\mu m$), audio (70–600 Hz), and visual ($400-700\mu m$) spectral bands, and UWB radar illumination (3–10 GHz).

2) There is a deep causal relationship between the

above sources of information. For example, gait and behavior/emotion pattern are correlated with possible possession of illegal concealed items [1], [41], [55].

3) Machine reasoning is the key operation in these technologies [62]. For example, an insobriety pattern can be reasoned upon analysis of thermal (infrared) measurements of face temperature, as well as body gesture and speech abnormalities. Such reasoning is performed under uncertainty, and, thus it is a probabilistic reasoning.

As the AI components for processing of heterogeneous data become more independent and sophisticated, the implications of their actions become more serious. Such AI tools performing actions on behalf of an operator could make errors that are difficult to "undo", for example, mis-identification of a person-of-interest. Moreover, for AI to operate effectively on the human's behalf, they might need confidential or sensitive information of the users such as financial details and personal contact information [11]. Trust becomes very important if an AI actions can cause their user physical, financial, or psychological harm. Thus, the users and the operators must be confident that the AI tools will do what they ask, and only what they ask. That is, a trusting relationship must develop between the humans and the AI tools. In the context of AI in identity management, trust means no longer controlling the AI tools directly, and letting the AI act on the human's behalf and accepting the risks this might entail.

Human acceptance of AI technology is determined by the combination of both trust and risk factors (e.g. Can we trust this machine decision?) and risk factors (e.g. How risky is this machine decision?) [2], [23], [58], [63]. The contributing factors include belief, confidence, experience, certainty, reliability, availability, competence, credibility, completeness, and cooperation [10]. Feelings of trust and risk can be established quite independently, and together they determine the intelligent tools success. Note that trust contributes to the AI tools acceptance, while risk contributes to its rejection. Trust and risk influence each other reciprocally [30]. It should be noted that Dempster-Shafer (DS) theory intrinsically contains the probabilistic ingredients for assessment of the system trust and risk. These possibilities are used, for example, for trust modeling in securing online reputation systems [34] and for risk validation in certificate security [26].

Computing the risk and trust under identity uncertainty has only been so far, partially studies. For example, effects of impersonation were studied in [61]. The risk countermeasures were studied in [6]. However, true AI-based decision making possibilities at the security checkpoint were not exploited. Few pilot projects on biometric-enabled AI technologies for identity management have been reported [22], [28], [33]. Technology-independent model of a checkpoint for border crossing security is given in Fig. 2 [62].

This work advances a technology further. We propose an approach based on the decomposition of the risk and trust assessment into a multi-state process based on the paradigms of 1) a multi-perception-action cycle (local and global), and 2) a cognitive computation concept (inspired by the cognitive

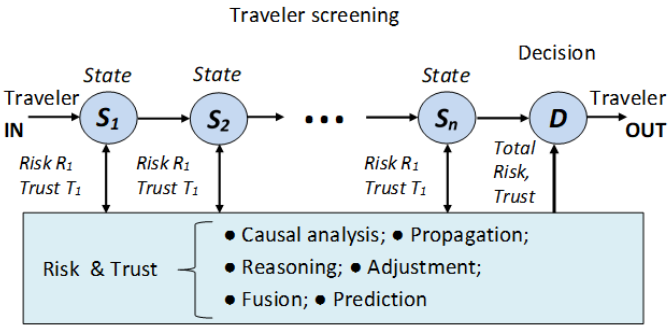


Fig. 2. Technology-independent model of a multi-state security checkpoint. The subject (traveler)'s risk is assessed using various mechanisms such as forward propagation (a process from effect to causes) and backward propagation (a process from causes to effect) of risk and trust through the states. Risk and trust are adjusted using their causal relationships. This is the core principle of traveler's risk mitigation.

dynamic systems [25]). The associated risks and trust are propagated from the first state (input data acquired using multiple cross-spectral sensors as well as prior data and any contextual data) to the last state (output data in the form of posterior probabilities and recommendations). At each intermediate state, the risks an trust are analyzed, updated, mitigated (via eliciting more information), and predicted. In legacy systems, risk assessment is performed by humans, such that data from ID readers and sensors is processed separately, and is supplied to a human operator to make a decision. In an AI-enabled decision support, this is enabled via a probabilistic reasoning mechanism. Modeling using probabilistic reasoning is a rational solution proposed in this paper.

This paper contributes to solving the three important challenges in identity management:

How to model security screening in conditions when the role of intelligent supporting tools becomes critical [56], [58]; We accept *Haykin's* concept of cognitive dynamical systems [25], and developed a multi-state cognitive identity management process;

How to measure risks and trust in the cognitive identity management [57], [60], [63]; We accept the *Pearl's* concept of the causality in cognitive dynamic systems [42] and developed the computational platform that combines various probabilistic measures of causal reasoning; and

How to exploit available approaches and resources for risk and trust analysis [12], [13], [54]; We accept the probabilistic notion of risk and trust [10], [47], we defined the fundamental operations on risk and trust, and demonstrate how they are implemented in the proposed computational model.

We revisit the risk and trust evaluation in complex systems, and define the cognitive security platform for identity management. We deploy a multi-state model of the identity management [62]. The core of the proposed cognitive platform is the novel inference engine. The prototype software implementation of this engine in available in [7].

II. Basic definitions, statements, and properties

The core research questions of our study are as follows: 1) Can we trust the cognitive identity management process? and 2) How risky are the decisions of the cognitive process? To answer those questions, the trust and risk in identity management should be defined first.

Definition 1: Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence [39].

Definition 2: Trust is the willingness of the trustor (evaluator) to take risk based on a subjective belief that a trustee (evaluatee) will exhibit reliable behaviour to maximize the trustor's interest under uncertainty (e.g., ambiguity due to conflicting evidence and/or ignorance caused by complete lack of evidence) of a given situation based on the cognitive assessment [10].

Definition 3: Trustworthiness is the degree to which an information system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats [39].

In our approach, risk, trust, and trustworthiness are measured in terms of probabilities. These general notions of risk and trust should be specified within the concept of identity management at a cognitive checkpoint.

A cognitive checkpoint is a complex dynamic system with the following elements of a cognitive system [25]: 1) perception-cycle (information gain about the state of identified person), 2) memory distributed across the entire system, 3) attention driven by memory to prioritize the allocation of available resources, and 4) intelligence driven by perception, memory, and attention; its function is to enable the control and decision-making mechanism to identify intelligent choices. These cognitive elements are distributed in the form of a multi-state multi-perception-cycle semi-automated model [62]. In addition, a cognitive checkpoint is a privacy-sensitive model [11], [14].

The goal of the cognitive semi-automated checkpoint is to answer the questions about (1) the risk of the decision (correct identification of a given individual or his/her behavioral patterns), and (2) the trust of the human operator in the system to the decision supplied by the AI (machine reasoning). This risk and trust assessment is based on multiple criteria such as reliability of sources, credibility of information, sensor precision, recognition algorithm performance etc. This assessment varies among the systems. Specifically, risk and trust assessment in a multi-state model is 1) distributed over states, 2) represented in causal relations, available for 3) propagation, 4) adjustment, 5) prediction, and 6) fusion. The mechanism enabling these operations is known as probabilistic inference called machine reasoning.

The key limitation factors of the risk and trust inference process are determined as follows. 1) The complexity of relationships between the states refers to various strategies to risk and trust assessment. Sources of information can have dual or multiple roles over the states. 2) Time limits of the operations place certain constraints on the sytem performance [28], [31], [45]. An example is a security problem known as the "bottleneck" and "traveler redress". Such problems are the reason why the screening process should be well synchronized with other resources. This is of critical importance, in particular, in the airport infrastructure. 3) Severity of consequences of the decisions made reflects the conceptual aspects of automated or semi-automated screening (decisions are made under incomplete, conflicting information, and the AI cognition is incomplete due to data or time constraints).

III. Fundamental operations on risk and trust

We consider a multi-state screening of an individual (Fig. 2) as a dynamic cognitive system that:

1) monitors the traveler data throughout the process of e-ID checking, face recognition, and continuously assess the risk using various sources such as behavioral biometrics, watchlist, e-interview results etc.,
2) updates its states based on the intelligence gathered via
   - human-machine interactions (e-interviewer),
   - results of the biometric traits recognition based on machine learning,
   - results of the concealed object detection (by adjusting radar illumination, in particular), and others.

Fig. 3 shows an example of the aforementioned functions in the context of the cognitive identity management for travelers crossing the borders:

- The traveler's identity management process is implemented in four states, S_1 (pre-screening based on Advanced Information), S_2 (ID validation), S_3 (Traveler authentication), and S_4 (Concealed object detection). Each state contains several sub-states. For example, the second state S_2 includes four sub-states $S_2^{(1)}$, $S_2^{(2)}$, $S_2^{(3)}$, and $S_2^{(4)}$.
- In a semi-automated system, the traveler can be directed to the manual control after each state, or can be directed to the next state.
- There are two types of dependency relationships that exist between states S_i and sub-states $S_i^{(j)}$: *intra-iteration* dependency (sub-states in the same loop), and *cross-iteration* (previous states) dependency.
- Each state S_i and sub-state $S_i^{(j)}$ is a part of the "Layered Security Strategy", a contemporary security doctrine [9], [29], [54].
- Each state S_i and sub-state $S_i^{(j)}$ generates risk and trust assessments for further processing and inference using operations such as propagation, causal analysis, reasoning, etc.

In our work, the taxonomy of risks is defined by the following fundamental operations:

1) State risk and trust assessment, such as the risk of the ID being fraudulent, or risks to privacy throughout the

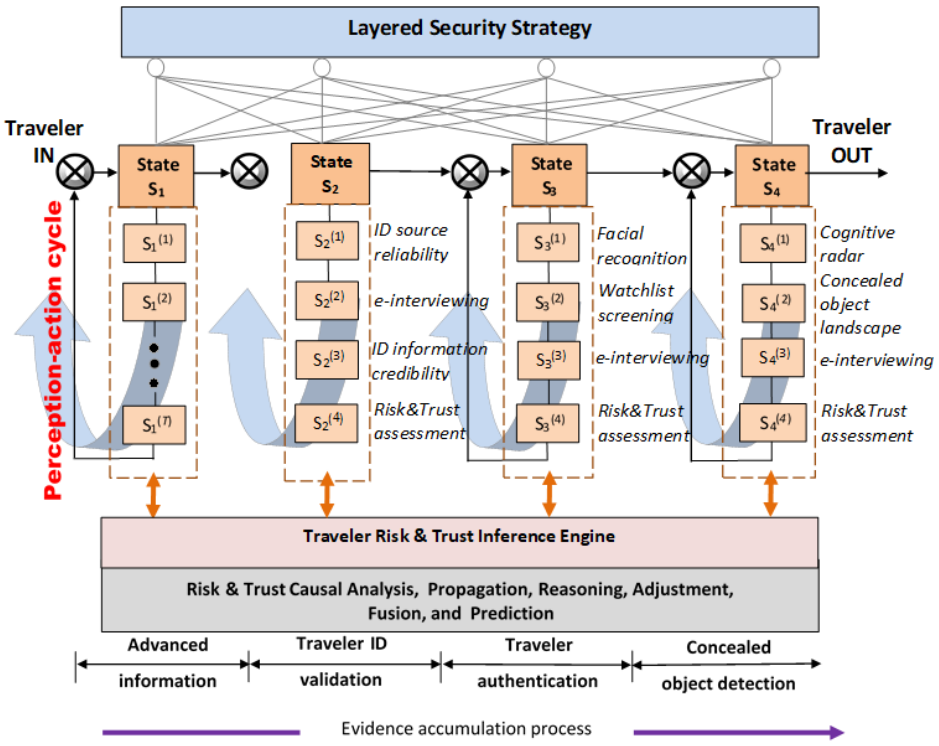


Fig. 3. Taxonomical view of the multi-state cognitive identity management process. Risks and trust are propagated from the first state (input) to the last state (output), and at each state their risk and trust status is causal analyzed, adjusted, fused, and predicted. Each state is represented by a perception-action cycle of sub-states.

e-interviewing. In modeling, each risk is represented by a corresponding probability distribution function.

2) Causal analysis of risks and trust is based on the "cause-effect" paradigm. In particular, Granger causality analysis is an advanced tool for this purpose [18], [48].

3) Risk and trust propagation. For example, if a person is on a watchlist, the risk of mis-identification or impersonation [61] is propagated through other states such as rik of mis-detection of a concealed item. The risk propagation problem was studied, in particular, as a multi-echelon supply chain problem in [40].

4) Risk and trust reasoning is the ability to form an intelligent conclusion or judgment using the risk and trust data. Causal reasoning is a judgment under uncertainty based on a causal probabilistic network. For example, assessed high risk to security based on a person's profiling does not always result in an overall high risk. Each state operates as a cognitive agent that makes a decision regarding the user risk and trust based on the specific resources such as previous experience (statistics) and observed information. The final risk assessment of the decision regarding the subject is negation, or consensus between the states (agents). The theoretical framework of such approach is known as the group decision making [59], [60].

5) Risk and trust adjustment aims at improving the confidence of the risk assessment. For example, non-match of facial images, one from an ID and another from a current probe image, may result in a high risk indicator, but can be later adjusted using the face aging (also called "template aging") factor.

6) Risk mitigation. In most scenarios, the risk can be lowered through the process of periodical re-assessment, as some risks can be downgraded to an acceptable level level and/or mitigated through the feedback and action as explained below.

7) Risk and trust prediction. In complex systems, meta-recognition, meta-learning, and meta-analysis can be used to predict the overall success (correct assessment of the risk and trust) or failure (incorrect one) of the system. The most valuable information for such risk assessment is in the "tails" of probabilistic distributions related to failures [15], [52].

IV. Perception-Action Cycle

The crucial element of a cognitive checkpoint is the risk perception-action cycle. A semi-formal description of a user risk and trust perception-action cycle is as follows:

$$\begin{bmatrix} \texttt{Person's} \\ \texttt{Risk \& Trust} \\ \texttt{assessment} \\ \texttt{[t+1]} \end{bmatrix} \equiv \begin{bmatrix} \texttt{Risk \& Trust} \\ \texttt{perception} \\ \texttt{state} \\ \texttt{[t]} \end{bmatrix} \times \begin{bmatrix} \texttt{Machine-Human, or} \\ \texttt{Machine-Machine} \\ \texttt{action} \\ \texttt{[t]} \end{bmatrix}$$

where a subject's risk assessment at time (level) $[t+1]$ is a result of a machine-human action over risk perception

resources (state) at time (level) $[t]$. Notion of the *perception-action cycle* is needed in terms of maximizing information gain about the individual computed from the observable data. For this, we adopted the perception-action cycle for a dynamic cognitive system [25].

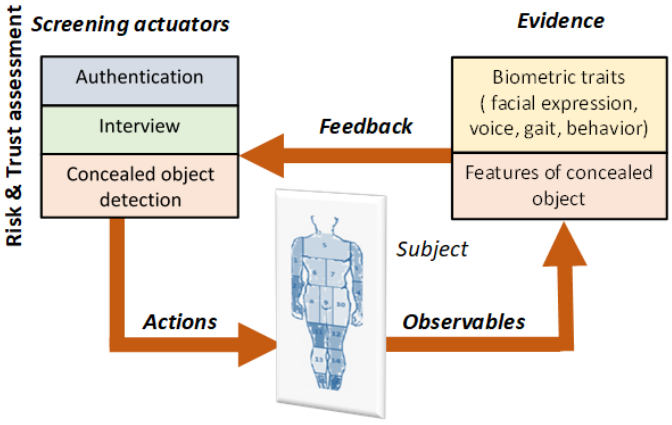


Fig. 4. Perception-action cycle is the core of a cognitive checkpoint. Each state in the model in Fig. 3 is represented as a perception-action cycle. In this loop, the traveler risk is assessed under available resources, and system risks and trust.

There are three key components of the perception-action cycle of the cognitive checkpoint (Fig. 4): *An individual* as a subject of multiple security measures applied in a supported infrastructure; *A screening actuator* that initializes execution of a security task or several security tasks; and *An evidence analyzer* that computes feedback information to the screening actuator.

Given an individual, the "screening actuator" initializes screening such as authentication (e.g. e-ID), human-machine interactions using e-interviewer, risk assessment (e.g. biometric-enabled watchlist and multi-cross information gathering), and concealed object detection (e.g. weapon and dangerous items). The observables refer to the results of security tasks execution. Feedback information computed by the "evidence analyzer" contains features such as: "failed authentication, additional data is needed"; next question should be generated; additional data is needed to complete risk assessment; and user action is needed to finalize concealed object detection (e.g. interview regarding orthopedic implants that are detected as dangerous items). Conceptually, the perception-action cycle reflects the user-adaptive properties based on a user model [35]. Note that the e-interview in the perception-action cycle is defined as the means to support the human-machine interactions using a spoken-dialog technology.

V. Inference Engine in Cognitive Identity Management

In this section, we describe a tool called an inference engine for modeling the multi-state cognitive identity management process illustrated in Fig. 3. This computational platform satisfied the requirements formulated in Section II in the form of statements and properties, and in Section III in the form of fundamental operations on risks and trust.

A. Probabilistic reasoning for decision under uncertainty

There are two kinds of operations in human identification process under uncertainty (Fig. 3): 1) operations within the system states that perform security tasks such as ID validation, individual identification, his/her risk assessment, as well as trust assessment of the risk sources, and 2) cross-state operations (causal analysis of risks and trust [56], [57], their propagation, fusion, reasoning and prediction [4], [40], [63]). Any of these operations can be implemented using probabilistic inference on a Bayesian network. The latter is a breakthrough concept introduced by Judea Pearl's and explained as follows: "*Causal reasoning is an indispensable component of human thought that should be formalized and algorithmitized toward achieving human-level machine intelligence*" [42].

The classic Bayesian networks operate only on one of possible projections of uncertainty, – point probabilities. However, there are other measure of uncertainty beyond the point probabilities. Combining causal reasoning with other uncertainty metrics was proposed, in particular, in [3], [44], a fuzzy Bayesian network has been developed. In [16], an interval metric was integrated within Bayesian networks. Reasoning mechanisms were extended with the belief Dempster-Shafer (DS) metric in [17], [46], [50]. The DS metric was extended in [51] and is known as Dezert-Smarandache (DSm) metric. We combine different uncertainty measures and place them on a unified reasoning platform [7]. This can be considered an expansion of the classic Bayesian network concept. In our approach, causal cognition refers to how a machine perceives, represents, and reasons about causal relationships of data:

$$\texttt{Causal Cognition} \equiv \begin{cases} \texttt{Point Probability,} & \text{Sec. VI-A;} \\ \texttt{Probability Interval,} & \text{Sec. VI-B;} \\ \texttt{DS Belief,} & \text{Sec. VI-C;} \\ \texttt{DSm Belief,} & \text{Sec. VI-D;} \\ \texttt{Fuzzy Probability,} & \text{Sec. VI-E.} \end{cases}$$

B. Taxonomical view of the uncertainty models

Our approach to handle uncertainty in the biometric-enabled identity management includes two components: (a) a graphical representation of a given scenario in the form of a causal network, and (b) a mechanism of uncertainty inference in different metrics. The causal network is a directed acyclic graph where each node in the graph denotes a unique random variable. A directed edge from node n_1 to node n_2 indicates that the value that is attained by n_1 has a direct causal influence on the value that is attained by n_2. As for metrics, we use the probability metric, probability intervals, the DS belief metric and its extension DSm, as well as the fuzzy probability metric.

Uncertainty inference requires data structures that will be referred to as *conditional uncertainty tables* (CUTs) in the general case. A CUT is assigned to each node in the causal network. Given a node n, the CUT assigned to n is a table that

is indexed by all possible value assignments to the parents of n. Each entry of the table is a conditional "uncertainty model" that varies according to the choice of uncertainty metric:

1) *Point probability:* Using the probability metric, the CUT is known as a Conditional Probability Table (CPT) and the causal networks are then referred to as Bayesian networks.

2) *Probability Interval:* Using the probability interval metric, the CUT is known as a Conditional Probability Interval Table (CPIT) and the causal networks are then referred to as probability interval Bayesian networks.

3) *DS Belief:* Using the DS metric, the CUT is known as a Conditional DS Table (CDST) and the causal networks are then referred to as DS Bayesian networks.

4) *DSm Belief:* Using the DSm metric, the CUT is known as a Conditional DSm Table (CDSmT) and the causal networks are then referred to as DSm Bayesian networks.

5) *Fuzzy Probability:* Using fuzzy probabilities, the CUT is known as a Conditional Fuzzy Probability Table (CFPT) and the causal networks are then referred to as fuzzy probability Bayesian networks.

Given a risk/trust assessment scenario, the proposed approach to its modeling includes the following steps:

Algorithm for multi-metric causal modeling

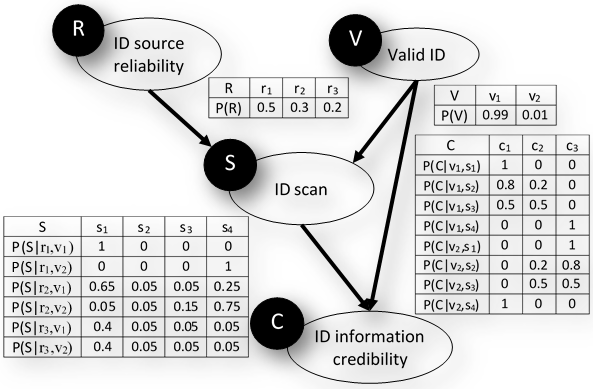
Step 1: Represent the risk/trust assessment scenario by a causal network.
Step 2: Assign CUTs in the appropriate metric to the nodes.
Step 3: Apply the observed evidence to the causal network and compute the posterior uncertainty model
Step 4: Make a decision based on a heuristic analysis of the posterior uncertainty model.

VI. Risk and Trust Inference Examples

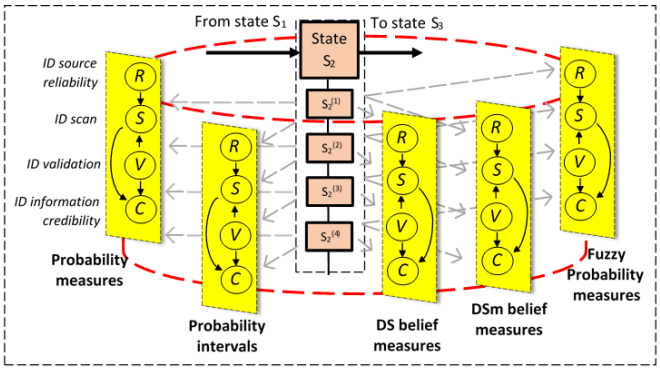
This section presents an example of an inference scenario that demonstrates how to measure risks and trust, and how they are propagated through a causal network to form a decision based on various metrics. Any scenario described by the multi-state model (Fig. 3) can be described and proceed using this inference engine. In the example below, the state S_2 (ID validation) from Fig. 3 is modeled. Due to the fuzziness of the variables involved and the lack of statistical data, the numerical values (probabilities and belief values) that populate the model are chosen arbitrarily for the sake of example and are not generated from real data.

A. Probabilistic measures using a Bayesian network

Consider the second state, S_2 (Fig. 3) and (b) available statistics for the CPTs the probabilities and belief values in this example have been arbitrarily chosen and are not generated from real statistics). Following the general strategy of causal network design, we, 1) Assign each state and sub-states of the model to nodes in a causal network (Table I), 2) Connect the nodes R, S, V, and C according to their causal relationships, 3) Construct the CPTs based on expert's or experimental knowledge, and 4) Make a decision; the belief network in Fig. 5 along with the CPTs provides a tool for probabilistic inference given various scenarios of ID validation. For example, $P(C|V = v_1, S = s_1)$ (denoted $P(C|v_1, s_1)$ in Fig. 3 for brevity) describes the scenario where a valid ID was authenticated on the first attempt. From the line $P(C|v_1, s_1)$, we can infer that the information credibility is certainly high in this scenario.



(a)



(b)

Fig. 5. (a) Causal network of the ID validation scenario in terms of risk and trust factors. (b) Each state of the identity management process is mapped into a unified causal networks over five metrics. This is an example of how the state S_2 'ID validation' (Fig. 3) with four sub-states defined in Table I can be mapped onto the uniform causal graph.

The Bayesian decision-making is based on evaluation of a *prior* probability given a *posterior* probability and *likelihood* (event happening given some history of previous events):

$$\overbrace{P(\texttt{Hypothesis}\,|\,\texttt{Data})}^{Prior} = \overbrace{P(\texttt{Data}\,|\,\texttt{Hypothesis})}^{Likelihood} \times \overbrace{P(\texttt{Hypothesis})}^{Posterior}$$

As an example of probabilistic inference using the Bayesian realization of the belief network, consider the following scenario: IF the reliability of the ID source is known to be 'low' and the credibility of the result to be 'high': $R = r_3$, and $C = c_1$, THEN what is the posterior probability that the ID is valid: $P(V = v_1|R = r_3, C = c_1)$. This scenario models a situation of conflict where an unreliable ID produces a credible out-

TABLE I
ASSIGNING STATES AND SUB-STATES OF THE MODEL TO A NODE IN THE CAUSAL NETWORK.

Assigning	Comment
$S_2^1 \rightarrow R$	The node 'ID source reliability' ($R \in \{r_1, r_2, r_3\}$) denotes the three level (r_1 ='high', r_2 ='medium', r_3 ='low') reliability of the e-passport/ID authentication, which depends on many factors such as: country of issue, number of defense levels in the document, life cycle history, type of the chip, type of biometric modality, type of encryption, and the type of RFID mechanism.
$S_2^2 \rightarrow V$	The node 'Valid ID' ($V \in \{v_1, v_2\}$) denotes whether the e-passport ID should pass the validation procedure (valid v_1) or not (invalid v_2). The 'valid' or 'invalid' state reflects the true state of the e-passport and not simply the opinion of the authentication machine.
$S_2^3 \rightarrow S$	The node 'ID scan' ($S \in \{s_1, s_2, s_3, s_4\}$) denotes the outcome of the authentication of the e-passport. The scan is subject to various unwanted effects such as the individual's mistakes in using the scanning device, scanner errors, as well as hidden reasons related to errors in the use of the database, conflicts of comparisons, and communication errors or delays. These effects are encoded in the form of the number of attempts at scanning the individual document; three attempts are allowed (s_1, s_2, s_3), after which the individual is directed to manual control (s_4). Ideally, if the individual's e-passport is invalid, they should always be directed to manual control.
$S_2^4 \rightarrow C$	The node 'ID Information credibility' ($C \in \{c_1, c_2, c_3\}$) describes the three level (c_1 ='high', c_2 ='medium', c_3 ='low') credibility of the outcome of the validation process. If the credibility of the validation process is known a priori, it can be used to compute posterior beliefs related to the validity of the individual document (node V).

come. The final result is $P(V = v_1|R = r_3, C = c_1) \approx 0.989$. It is very likely that the ID was valid.

Essential features of probabilistic measures of evidential reasoning using Bayesian networks are as follows: 1) they represent the certainty in an attribute-value as a point probability, and 2) they require complete knowledge of both prior and conditional probabilities, which might be difficult to determine in practice.

B. Probability interval measures

Theory from [16] describes operations for creating marginal probability interval distributions and conditional probability interval distributions from joint probability interval distributions. Joint probability interval distributions can be formed from the probability interval distributions of independent variables. For the current example, an uncertainty radius of 0.1 will be extended around each probability value, except to where the probability is decisively 0 or 1. For example, the probabilities for node V will become $P(V = v_1) = [0.89, 1]$, $P(V = v_2) = [0, 0.11]$.

As an example of inference using probability intervals, the same scenario will be considered: `IF` the reliability of the ID source is known to be 'low' and the credibility of the result to be 'high': $R = r_3$, and $C = c_1$, `THEN` what is the posterior probability that the ID is valid: $P(V = v_1|R = r_3, C = c_1)$. The final result is: $P(V = v_1|R = r_3, C = c_1) = [0.574, 1]$. This interval implies that within the flexibility allowed by the probability intervals, the posterior probability of the ID being valid can be low as 0.574. It should also be noted that the posterior probability interval will always contain the probability value produced by the Bayesian realization of the belief network (which in this case was 0.989). Probability interval measures partially improve the Bayesian technique, but does not have a convenient representation for ignorance or uncertainty.

C. DS belief measures

DS evidential theory has been considered when an incomplete probabilistic model is created, i.e. when the prior probabilities and likelihood functions are unknown [17]. In contrast, the Bayesian inference does not have this allowance. A description of DS theory can be found in [46]. The procedure will be the same except for the CUTs. The approach here uses theory from [17], [20]. However, an alternative approach has been developed [50]. As an example of inference using the DS realization of the belief network, the same scenario is used: `IF` the reliability of the ID source is known to be 'low' and the credibility of the result to be 'high': $R = r_3$, and $C = c_1$, `THEN` what is the posterior belief and plausibility that the ID is valid: Bel$(V = v_1|R = r_3, C = c_1)$, Pl$(V = v_1|R = r_3, C = c_1)$. The final result is: Bel$(V = v_1|R = r_3, C = c_1) \approx 0.878$ and Pl$(V = v_1|R = r_3, C = c_1) \approx 0.951$. Together, these two values form the interval of probability values $[0.878, 0.951]$. This interval implies that it is very likely that the ID was valid. Unlike the Bayesian network realization of the belief network, the DS realization of the belief network produces a range of probability values. Unlike probability intervals however, this range is heuristic and may not denote an objectively quantifiable value.

It should also be noted that the range of probability values produced by the DS realization of the belief network (which in this case is $[0.878, 0.951]$) does not necessarily contain the probability value produced by the Bayesian realization of the belief network (which in this case was 0.989).

Fig. 6 explains the low bound, or belief, and upper bound, or plausibility. It shows what proportion of evidence is truly of a proposition and what proportion comes merely from ignorance:

<DS uncertainty interval>= [`Belief, Plausibility`]

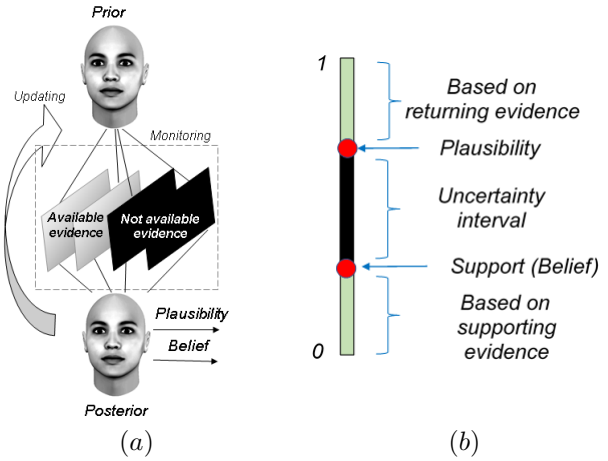


Fig. 6. The DS uncertainty interval. The DS technique can handle uncertainty, or ignorance, ythat is, lack of knowledge of the complete probabilistic model required for Bayesian inference.

where the lower bound is the belief confidence, and the upper bound is the plausibility confidence. Note that the DS formulation of a problem collapses into the probabilistic one using Bayesian network when the uncertainty interval is zero.

D. DSm belief measures

DSm theory is a generalization of DS theory. A description of the DSm approach can be found, in particular, in [51]. The DSm technique of plausible and paradoxical reasoning deals with high conflicting uncertainty and imprecise sources of evidence. For instance, data can be represented using a formal notion of reliability (refers to quality) and importance (refers to subjective preferences).

As an example of probabilistic inference using the DSm realization of the belief network, the same scenario is used: `IF` the reliability of the ID source is known to be 'low' and the credibility of the result to be 'high': $R = r_3$, and $C = c_1$, `THEN` what is the posterior belief and plausibility that the ID is valid: $\text{Bel}(V = v_1|R = r_3, C = c_1)$, $\text{Pl}(V = v_1|R = r_3, C = c_1)$ The final result is: $\text{Bel}(V = v_1|R = r_3, C = c_1) \approx 0.878$ and $\text{Pl}(V = v_1|R = r_3, C = c_1) \approx 0.951$. Together, these two values form the interval of probability values $[0.878, 0.951]$.

E. Fuzzy probability measures

The theory of fuzzy probabilities that will be used in this experiment is described in [3], [44]. A fuzzy probability consists of a center value that acts as a normal probability, and a lower and upper limit that contains the center value. The interval formed by the lower and upper limit is not subject to the same requirements as the probability intervals from [16]. For example, the first line of the CFPT corresponding to node C (ID information credibility) is shown below

$$\Pr(C|V = v_1, S = s_1) = \begin{cases} (1,1,1), & C = c_1(\text{high}); \\ (0,0,0), & C = c_2(\text{medium}); \\ (0,0,0), & C = c_3(\text{low}). \end{cases}$$

As an example of probabilistic inference using fuzzy probabilities, the same scenario will be considered: `IF` the reliability of the ID source is known to be 'low' and the credibility of the result to be 'high': $R = r_3$, $C = c_1$, `THEN` what is the posterior probability that the ID is valid: $\Pr(V = v_1|R = r_3, C = c_1)$. The calculations are performed using theory that is described in [44]. The final result is: $P(V = v_1|R = r_3, C = c_1) = (0.113, 0.989, 8.146)$. This fuzzy probability implies that within the flexibility allowed by the fuzzy probabilities, the posterior point probability can be as low as 0.113. Despite an upper bound that exceeds 1, the true posterior point probability still cannot exceed 1. The upper bound of 8.146 simply shapes the membership function of the fuzzy posterior probability inside of the interval [0, 1].

F. Inference summary

Table II provides a summary of inference engine operation for the scenario of the ID validation. In the first column of Table II, five uncertainty metrics are placed; in the second and third column, computing probabilities of decision on Valid ID and Invalid ID, respectively, are reported. In the fourth column, we refer the theory source of an uncertainty metric. In the last line, we emphasize that we infer the same scenario that is represented by the common causal graph (Fig. 5) but for reasoning was used five uncertainty metrics; this mechanism is placed on the software platform [7].

These five different uncertainty projections, or interpretations, strongly suggest that `' ID is Valid given the evidence 'low' ID source reliability and 'high' ID information credibility'`. Note, that DS and DSm did not discover the data conflict features, but this may not be the case in general. Fig. 7 provides a graphical interpretation of the results reported in Table II.

This inference summary reflects that initial risks and trust defined in terms of 'low' ID source reliability and 'high' ID information credibility were fused by the reasoning mechanism and reported in different uncertainty metrics.

VII. Summary, Conclusion, and Future Work

Deep embedding of the AI into identity management systems is an emerging trend. What was previously human-human interaction becomes human-machine and even machine-machine interactions with delegating decision-making to autonomous agents. The embodiment of this trend in our study is a proposed cognitive platform. In these new scenarios, risk and trust factors become the important issue for technology and policy developers, AI operators and users. This work contributes to solutions to this challenge, and proposes a multi-state cognitive identity management platform and inference engine that are able to predict various unwanted and often unknown effects in terms of risk and trust. We demonstrate it on a sample scenario describing the heterogeneous data management (document validity, contextual information and biometrics). The key conclusions are as follows:

TABLE II

A COMPARISON OF THE RESULTS OF THE INFERENCE EXAMPLE BASED ON DIFFERENT UNCERTAINTY METRICS FOR VALID ID ($V = v_1$) AND INVALID ID ($V = v_2$) SCENARIOS USING 'LOW' ID SOURCE RELIABILITY ($R = r_3$) AND 'HIGH' ID INFORMATION CREDIBILITY ($C = c_1$)

Uncertainty Metric	**Valid ID** $P(V = v_1 \mid r_3, c_1)$	**Invalid ID** $P(V = v_2 \mid r_3, c_1)$	**Comment**
1. Probabilities	0.989	0.011	Inference on classic Bayesian network
2. Probability Intervals	[0.574, 1.000]	[0.000, 0.426]	Based on theory from [16]
3. DS Belief Plausibility	[0.878, 0.951]	[0.049, 0.122]	Based on theory from [17], [46]
4. DS**m** Belief Plausibility	[0.878,0.951]	[0.049,0.122]	Based on theory from [51]
5. Fuzzy Probabilities	(0.113,0.989,8.146)	(0.000, 0.011, 0.742)	Based on theory from [3], [44]
Common causal network framework of the ID validation scenario in terms of risk and trust [7]			

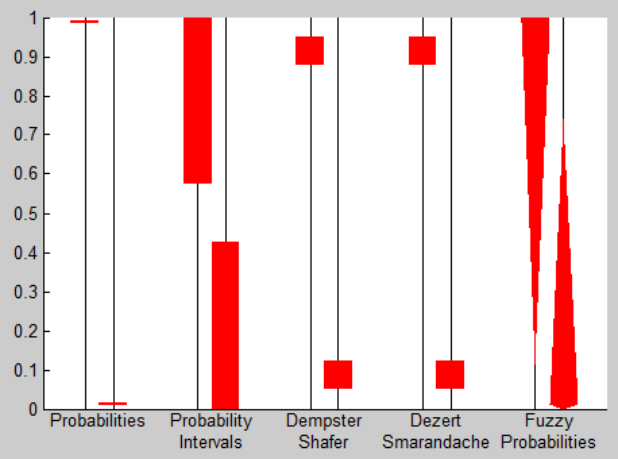


Fig. 7. A graphical interpretation of the inference operation for the ID validation scenario in five uncertainty metrics (Table II). The posterior uncertainty quantities over V (valid ID) given the evidence $R = r_3$ ('low' ID source reliability) and $C = c_1$ ('high' ID information credibility). For each metric, the left column corresponds to $V = v_1$ (valid ID) and the right column corresponds to $V = v_2$ (invalid ID).

1) A multi-state model called a cognitive dynamic system is useful for representation of the identity management process.
2) A computational platform of this system is based on probabilistic reasoning build upon a causal network with a variety of probability measurements. It provides a wide range of tools for risk and trust assessment, as well as prediction via inference on the causal network.

In addition, the proposed model (Fig. 3 and Fig. 4) and the inference engine can be used for estimation of technology gaps. This is required to identify whether it is possible to achieve the design goals given the available resources and technologies [21].

The focus of our future work is the cognitive biases in machine reasoning in a multi-state identity management process. The biases lead to faults in the reasoning processes. The resulting risk and trust decisions may violate the commonly accepted normative principles. The analogous biases in human reasoning are the base for this study. An example is the overconfidence bias when eliciting probability distributions from experts in risk analysis [36]. The future work also includes an extension of the inference engine. In particular, it will benefit from integrating the causal analysis of risks and trust using Granger approach [8], as well as from a fusion of data represented by its probabilistic distribution (known as copula [5]).

Acknowledgments. This Project was partially supported by the European Union's Horizon 2020 research [13]; Natural Sciences and Engineering Research Council of Canada (NSERC) through grant "Biometric-enabled Identity management and Risk Assessment for Smart Cities", and Defence Research and Development Canada (DRDC). Dr. *Shawn C. Eastwood* is acknowledged as a developer of the initial version of the multimetric inference software DS-BN v02. The authors also acknowledge the anonymous reviewers for their valuable recommendations on improving the paper.

REFERENCES

[1] M. Abouelenien, *et al.,* Detecting Deceptive Behavior via Integration of Discriminative Features From Multiple Modalities, *IEEE Trans. Inf. Forensics and Security*, vol. 12, no. 5, 2017, pp. 1042–1055.
[2] D. Anand and K. K. Bharadwaj, Pruning trust–distrust network via reliability and risk estimates for quality recommendations, *Social Network Analysis and Mining*, vol. 3, 2013, pp. 65–84.
[3] J. F. Baldwin and E. D. Tomaso, Inference and learning in fuzzy Bayesian networks, *Proc. 12th IEEE Int. Conf. Fuzzy Syst.*, vol. 1, 2003, pp. 630–635.
[4] C. Baudrit, D. Dubois, and D. Guyonnet, Joint Propagation and Exploitation of Probabilistic and Possibilistic Information in Risk Assessment, *IEEE Trans. Fuzzy Systems,* vol. 14, no. 5, 2006, pp. 593–608.
[5] T. Bedford, A. Daneshkhah, and K. J. Wilson, Approximate Uncertainty Modeling in Risk Analysis with Vine Copulas, *Risk Analysis*, vol. 36, no. 4, 2016, pp. 792–815.
[6] B. Biggio, G. Fumera, G. L. Marcialis, and F. Roli, Statistical meta-analysis of presentation attacks for secure multibiometric systems, *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 39, no. 3, 2017, pp. 562–575.
[7] Dempster-Shafer Bayesian Network Inference Package (DS-BN) v.02, v.03, Biometric Technologies Laboratory, University of Calgary, 2019, http://www.ucalgary.ca/btlab/Software
[8] S. Cekic, D. Grandjean, and O. Renaud, Time, frequency, and time-varying Granger-causality measures in neuroscience, *Statistics in Medicine*, vol. 38, 2018, pp. 1910–1931.
[9] S. Chatterjee, S. C. Hora, and H. Rosoff, Portfolio Analysis of Layered Security Measures, *Risk Anal.,* vol. 35, no. 3, 2015, pp. 459–475.
[10] J.-H. Cho, K. Chan, and S. Adali, A Survey on Trust Modeling, *ACM Computing Surveys*, vol. 48, no. 2, Article 28, 2015.
[11] G. G. Clavell, Protect rights at automated borders *Nature,* vol. 543, Issue 7643, March, 2017.
[12] K. Crockett, *et al.,* Do Europe's borders need multi-faceted biometric protection? *Biometric Tech. Today*, vol. 7, 2017, pp.5–8

[13] H2020 Intelligent SMART Border Control (iBorderCtrl), https://www.iborderctrl.eu/

[14] K. Crockett, S. Goltz, and M. Garratt, GDPR Impact on Computational Intelligence Research, *Proc. Int. J. Conf. Neural Net.,* 2018, pp. 1–7.

[15] A.C. Davison and R. Huser, Statistics of Extremes, *Annu. Rev. Stat. Appl.*, vol. 2, 2015, pp. 203–235.

[16] L. M. De Campos, J. F. Huete, and S. Moral, Probability intervals: a tool for uncertain reasoning, *Int. J. of Uncertainty, Fuzziness and Knowledge-Based Syst.*, vol. 2, no. 2, pp. 167–196, 1994.

[17] F. Delmotte and P. Smets, Target identification based on the Transferable Belief Model interpretation of Dempster-Shafer model, *IEEE Trans. Syst., Man and Cyber., Part A: Syst. and Humans*, vol. 34, no. 4, 2004, pp. 457–471.

[18] F. Eberhardt, Introduction to the foundations of causal discovery, Int. J. Data Sci. Anal., 2017, 3, pp. 81–91.

[19] S. Eastwood, V. Shmerko, S. Yanushkevich, *et al.,* Biometric-enabled authentication machines: A survey of open-set real-world applications, *IEEE Trans. Human-Machine Syst.*, vol. 46 , no. 2, 2016, pp. 231–242.

[20] S. Eastwood, and S. Yanushkevich, Risk Assessment in Authentication Machines, In: R. Abielmona, *et al.,* Eds, *Recent Advances in Comput. Intell. in Defense and Security*, Springer, 2016, pp 391–420.

[21] S. Eastwood, K. Lai, S. N. Yanushkevich, R. Guest, and V. Shmerko, Technology Gap Navigator: Emerging Design of Biometric-Enabled Risk Assessment Machines *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Germany, 2018, pp. 1–5.

[22] European Union: Technical Study on Smart Borders, *EU, European Commission*, B-1049, Brussels, 2014.

[23] N. Feng, H. J. Wang, and M. Li, A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis, *Information Sciences*, vol. 256, 2014, pp. 57–73.

[24] S. W. Harmer, N. Bowring, D. Andrews, *et al.,* A Review of Nonimaging Stand-Off Concealed Threat Detection with Millimeter-Wave Radar, *IEEE Microwave Magazine*, Jan./Feb., 2012, pp. 160–167.

[25] S. Haykin, *Cognitive Dynamic Systems (Perception-Action Cycle, Radar, and Radio)*, New York: Cambridge University Press, 2012.

[26] M. F. Hinarejos, *et al.*, RiskLaine: A Probabilistic Approach for Assessing Risk in Certificate-Based Security, *IEEE Trans. Inf. Forensics and Security*, vol. 13, no. 8, 2018, pp. 1975–1988.

[27] IATA (International Air Transport Association): Checkpoint of the future. Executive summary. 4th Proof. 2014.

[28] IATA (International Air Transport Association): Automated Border Control. Implementation Guide, 2015.

[29] B. A. Jackson and T. LaTourette, Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries, *J. Air Trans. Manag.* vol. 35, 2015, pp. 26–33.

[30] G. Kim and H.Koo, The causal relationship between risk and trust in the online market place: A bidirectional perspective, *Computers in Human Behavior*, vol. 55, 2016, pp. 1020–1029.

[31] R. D. Labati, A. Genovese, E. Munoz, V. Piuri, F. Scotti, and G. Sforza, Biometric Recognition in Automated Border Control: A Survey, *ACM Comp. Surv.*, vol.49, no.2, 2016, pp. A1-A39.

[32] K. Lai, S. Yanushkevich, V. Shmerko, and S. Eastwood, Bridging the Gap Between Forensics and Biometric-Enabled Watchlists for e-Borders, *IEEE Comput. Intell. Mag.*, vol. 12, no. 1, 2017, pp. 17–28.

[33] K. Lai, S. Eastwood, W. Shier, S. Yanushkevich, and V. Shmerko, Mass Evidence Accumulation and Traveler Risk Scoring Engine in e-Border Infrastructure, *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 10, 2018, pp. 3271–3281.

[34] Y. Liu, *et al.*, Securing Online Reputation Systems Through Trust Modeling and Temporal Analysis, *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 6, 2013, pp. 936–948.

[35] G. S. Martins, L. Santos, and J. Dias, BUM: Bayesian User Model for Distributed Learning of User Characteristics From Heterogeneous Information, *IEEE Trans. Cognitive and Developmental Syst.*, vol. 11, no. 3, 2019, pp. 425–434.

[36] G. Montibeller and D. von Winterfeldt, Cognitive and Motivational Biases in Decision and Risk Analysis,*Risk Analysis*, Vol. 35, No. 7, 2015, pp. 1230–1251.

[37] A. G. Nikolaev, A. J. Lee, and S. H. Jacobson, Optimal Aviation Security Screening Strategies With Dynamic Passenger Risk Updates, *IEEE Trans. Intell. Transp. Syst.,* vol. 13, no. 1, 2012, pp. 203–212.

[38] N. Nikolova and T. Thayaparan, Ultra-Wideband (UWB) high-resolution radar for concealed weapon detection, Technical Report TR 2013-160, Defence Research and Development Canada, 2014.

[39] National Institute of Standards (NIST), Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Revision 5, 2017.

[40] R. Ojha, A. Ghadge, M. K. Tiwari, and U. S. Bititci, Bayesian network modelling for supply chain risk propagation, *Int. J. Production Research,* Vol. 56, No. 17, 2018, pp. pp. 5795–5819

[41] J. O'Shea, *et al.,* Intelligent Deception Detection through Machine Based Interviewing, *Proc. Int. Joint Conf. Neural Networks,* 2018, pp. 1–8

[42] J. Pearl, The Seven Tools of Causal Inference, with Reflections on Machine Learning, *Communication of the ACM,* vol. 62, no. 3, 2019, pp. 54–60.

[43] B. A. Rajoub and R. Zwiggelaar, Thermal Facial Analysis for Deception Detection *IEEE Trans. Inf. Forensics and Security,* vol. 9, no. 6, 2014, pp. 1015–1023.

[44] J. Ren, I. Jenkinson, J. Wang, *et al.,* An Offshore Risk Analysis Method Using Fuzzy Bayesian Network, *J. Offshore Mech. and Arctic Eng.*, vol. 131, no. 4, 2009, pp. 041101-1–12.

[45] J. J. Robertson, R. M. Guest, S. J. Elliott, and K. O'Connor, A Framework for Biometric and Interaction Performance Assessment of Automated Border Control Processes, *IEEE Trans. Human-Mach. Syst.,* vol. 47, no. 6, 2017, pp. 983–993.

[46] G. Shafer, P. P. Shenoy, and K. Mellouli, Propagating belief functions in qualitative Markov trees, *Int. J. Approx. Reasoning*, vol. 1, no. 4, 1987, pp. 349–400.

[47] J. Shortridge, T. Aven, and S. Guikema, Risk assessment under deep uncertainty: A methodological comparison, *Reliab. Eng. and Syst. Saf.,* vol. 159, 2017, pp. 12–23.

[48] P. Spirtes and K. Zhang, Causal discovery and inference: concepts and recent methodological advances, *Appl. Inform.,* 2016, 3, issue 3.

[49] M. G. Stewart and J. Mueller, Risk and economic assessment of U.S. aviation security for passenger-borne bomb attacks, *J. Transp. Secur.,* 2018, published online.

[50] C. Simon, P. Weber, and A. Evsukoff, Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis, *Reliab. Eng. and Syst. Safety* vol. 93, 2008, pp. 950–963.

[51] F. Smarandache, J. Dezert, and J.-M. Tacnet, Fusion of sources of evidence with different importances and reliabilities, *Proc. Conf. Inf. Fusion*, Edinburgh, 2010.

[52] M. Stehlik *et al.,* On the favorable estimation for fitting heavy tailed data, *Comput. Stat.*, vol. 25, 2010, pp. 485–503.

[53] T. Truong, and S. Yanushkevich, Generative Adversarial Network for Radar Signal Generation, *Int. Joint Conf. Neural Networks (IJCNN)*, Budapest, 2019, pp.1–6.

[54] Transportation Security Administration, *Layers of Security,* 2013. Available at: http://www.tsa.gov/about-tsa/layerssecurity

[55] N. Twyman, *et al.,* Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals, *J. Manag. Inf. Syst.,* vol. 31, no. 3, 2014, pp. 106–137.

[56] T. Van hamme, D. Preuveneers, and W. Joosen, Managing distributed trust relationships for multi-modal authentication, *J. Information Security and Applications*, vol. 40, 2018, pp. 258–270.

[57] Y. Wang and M. P. Singh, Evidence-Based Trust: A Mathematical Model Geared for Multiagent Systems, *ACM Trans. Autonomous and Adaptive Systems*, vol. 5, no. 4, Article 14, 2010.

[58] M. Whittaker, *et al.*, AI Now Report, New York University, 2018, https://ainowinstitute.org/AI_Now_2018_Report.pdf

[59] J. Wu, F. Chiclana, H. Fujita, and E. Herrera-Viedma, A visual interaction consensus model for social network group decision making with trust propagation, *Knowledge-Based Systems*, vol. 122, 2017, pp. 39–50.

[60] X. Xu, *et al.,* A Risk Elimination Coordination Method for Large Group Decision-Making in Natural Disaster Emergencies, *Human and Ecol. Risk Ass.*, vol. 21, 2015, pp. 1314–1325.

[61] S. N. Yanushkevich, S. W. Eastwood, and S. Samoil, Taxonomy and modelling of impersonation in e-border authentication, *Proc. Int. Conf. Emerging Security Technologies,* Germany, 2015, pp. 38–43

[62] S. Yanushkevich, K. Sundberg, N. Twyman, R. Guest, and V. Shmerko, Cognitive checkpoint: Emerging technologies for biometric-enabled watchlist screening, *Computer and Security,* vol. 85, 2019, pp. 372–385.

[63] R. Zhang and Y. Mao,Trust Prediction via Belief Propagation, *ACM Trans. Information Systems*, vol. 32, no. 3, Article 15, 2014.