The Alan Turing Institute

Architecting our Future

Insights from the Inaugural Trustworthy Digital Identity Conference

December 2021

Contents

A word from the conference chairs

As the world adapts to an increasingly digital and global society, many forms of digital Identity are evolving at pace, employing a multitude of technologies, and yielding a lived experience that reveals their growing significance. The Alan Turing Institute's inaugural Trustworthy Digital Identity Conference offered a snapshot of that lived experience and showcased examples of the global effort to architect a future that can be informed by their impact on lives, communities and the relationships people develop with the organisations that they interact with every day. Staged amidst a global pandemic that has not only been a catalyst for digital capabilities, but also rendered traditional means of verifying the right to receive public benefits, buy or rent a home, or start a new job more difficult than ever, the event marked the beginning of an important conversation.

Seats were made available to 100 participants identified as actively working in digital identity. Coming from academia (38%), industry (29%), government and the third sector (19%), people joined and actively contributed perspectives from 29 countries that span the globe from Brazil to New Zealand.

Sessions covered projects that explore new business and service-delivery models; attitudes toward biometrics; changing relationships between governments and their citizens; opportunities to develop more representative Artificial Intelligence and more. Many put an emphasis on the challenges faced by the most vulnerable or marginalised in society, and advanced lessons to be learned from the profiles and particular challenges faced by migrating populations. Underlining an important role of research in this area, the day's conversation brought focus to both the unanticipated consequences and risks that are being realised through the lived experience, and the opportunities for collaboration that can help everyone move forward.

In reviewing insights from each session, this conference report offers a view of how the global conversation is developing through efforts to define what good looks like; assure inclusivity and advance varied technical and system design opportunities. If there was a stand-out theme for the day, it was that context matters: there is no one approach that can be said to be appropriate for all communities or applications. The artificial intelligence being imbedded into these systems should draw on data sets relevant to the use case and systems should be designed around specific societal needs.

It is our sincere hope that in bringing so many perspectives together, this conversation will help to architect that informed future and in doing so help society move toward the fairer, more inclusive world that so many are working to achieve.

Professor Carsten Maple,
Professor Jon Crowcroft, Dr Mark Hooper

What does good look like?

"We are considering the humanity side of things and the inclusivity side of things far before we start to think about the technology that can help solve these problems."

Dr Louise Maynard-Atem, research lead Women in Identity (WID)

Many approaches to digital identity systems have emerged to meet sector, government, humanitarian, commercial, and even individual objectives. Drawing on broad programmes of consultation with citizen or constituent groups, the presentations offered perspectives from government, practitioners and the humanitarian sector about the definition of mechanisms to guide deployment and design of digital ID.

One government's perspective

Hannah Rutter, Deputy Director, Digital Identity and Secure Connected Places, Government of the United Kingdom (UK) keynoted the conference with an overview of the proposed UK Digital Identity & Attributes Trust Framework for the development of digital identity products. The UK is an example of growing interest on the part of national governments around the world in digital ID development. Rutter pointed out that a need was made obvious when more than 1.4 million citizens could not present the credentials needed to access support during the pandemic.

"We want to make sure this is not something that is only available to people who have high-end smartphones, who are already able to navigate the digital economy successfully. We want anyone who wishes to, to be able to use digital products, and indeed the great win that we see is to make it easier for those who currently struggle to prove their identity."

By setting out principles and measures within a framework, the UK is looking to industry to develop the technology according to expectations that underline security, data protection and ethical requirements, and ensure the person using it can trust it. Goals outlined included the opportunity to improve not just access to services, but also legacy processes that rely on physical documents. "At the moment in the UK, if you want to prove something about yourself, you tend to present an array of documents: your passport, driving license, utility bills, and all of that contains a lot of data about you, probably more than the person checking it needs to see," she said, adding the desire for digital ID to facilitate proportional solutions should be tuned to given scenarios. "The level of trust you need to be able to say, I am over 18 and I can buy this bottle of wine is a different level of trust to buy a house."

Citing her government's research, Rutter stated aims to save £800 million a year for UK businesses, if they can "get it right" and encourage widespread use of digital identity and attribute products. Getting it

right in the UK, which has a long history of resisting national ID cards, must draw on societal values and context: "We often have pointed to us examples of some of the Nordic, some of the other countries that have successfully created digital identity solutions. They are exciting, but they are based on systems that we do not have here because we do not have national identity cards or datasets," she said.

Practitioners Perspective

With their initiative to write a Code of Conduct, Women in Identity (WID), a volunteer-run, international not-for-profit membership organisation, seeks to help organisations and developers understand where exclusion and bias can creep into the design process of new identity solutions. With digital identity systems becoming the gatekeeper to financial services, online banking, e-commerce and insurance, this initiative was described as a response to the potential for technologies within digital identity systems to entrench, and exacerbate, the exclusionary and biased practises that exist in society.

Dr Louise Maynard-Atem, research lead Women in identity (WID) reviewed this project within her session ***Inclusion by design: Creating digital identities that work for all***. She opened with two requirements in any systems development: an understanding of the problems systems are being designed to address; and an understanding of the people the systems are designed to serve. "We are considering the humanity side of things and the inclusivity side of things long before we started to think about the technology that can help solve these problems."

"We've actually had very little guidance on how best to tackle inclusion and bias in the digital identity sector," Maynard-Atem pointed out. "There is a huge amount of really valuable work that talks about the problem from various different angles. There is very little that then says, how do we go about actually implementing change."

The project ambitions are to identify the decision points that lead to biased or exclusionary outcomes, and develop a code of conduct with principles that

can be overlayed on to existing product development design processes or lifecycles. Working with research partner Caribou Digital with the support of funding and sponsors that include The Omidyar Network, GBD, Mastercard and the Royal Bank of Canada, they are currently reviewing the assumptions and data that are being fed into identity systems within financial services, to flag where challenges are emerging in the development process. The scope also includes foundational econometric modelling, to measure the cost of exclusion and identify relevant datasets for benchmarking this over time.

"Organisations can go through the checklist and think about what they need to be going through when they're developing a new product or service so at every point that bias has crept into the process they are able to course correct for that," she explained, pointing to examples of exclusion prevalent in systems predicated on existing, usually government- issued identity documents, and algorithms with higher rates of false positives for particular ethnic groups.

Recommendations for the humanitarian sector

A collaborative project from the International Federation of Red Cross and Red Crescent Societies (IFRC) to review the impact of digital identity use in the humanitarian support of migrant populations produced five recommendations for humanitarian organisations published in June. Discussing highlights in their session ***Defining digital identities for humanitarian action in migration***, IFRC 's Joseph Oliveros and Nadia Khoury acknowledged that they are trusted because of who they are, which drives a sense of accountability for security and privacy alongside broader requirements for protecting against other risks that may be introduced with digital systems.

Reflecting the experience of various groups of people on the move within individual countries and across borders, Report Author Nadia Khoury emphasised that humanitarian organisations' desire to "remain accountable for our work and the people that we attend to," is frustrated by the fact that access to services, which range from immediate, emergency assistance and attending really basic needs to services that have a stabilisation or integration focus tend to be conditioned on migrants sharing or proving their identity.

"Of course, humanitarian agencies always try to assist the most vulnerable … however, we did find that this requirement creates challenges in providing services to people who really need them. This calls for reflection from humanitarian organisations for the reasons for which identity data is collected and processed, and how this need is balanced against migrants right to privacy and the overriding humanitarian requirement of the most vulnerable to be assisted."

Recommendations started with a call for a long-term vision for the use of digital identities and advocated a consortia model for the delivery of digital ID. The model would be facilitated by technical interoperability and clear governance structures that incorporate relevant expertise in the sector's advisory and decision-making functions. The idea is to develop a capacity to define common aims across agencies that can underpin more cohesive support, while also relieving the burden of costly and time-consuming registration: "Ideally, we would want to avoid a constant collection of personal data for people who go through points of attention and allow for a more dignified treatment for those migrants," she said.

The speakers highlighted the need for a highly contextual interpretation of inclusivity that caters to varying levels of literacy, including digital literacy, language, cultural and personal diversity, gender age and varying levels of access to information. "Access to information is almost equal to access to humanitarian assistance," stated Khoury.

Oliveras added that it also calls for careful consideration of the vulnerabilities of migrants acknowledging that in some cases, "vulnerability might render someone unsuitable for digital identity."

The relationships being defined by digital ID

"It is because the infrastructure needs to be serviced and has become a policy area of its own, rather than being seen as a mechanism of improving service delivery, so you get that flipside of the policy priorities."

Katelyn Cioffi, research scholar, Center for Human rights and Global Justice, NYU School of Law.

Research scholar, Katelyn Cioffi, at the NYU School of Law's Center for Human rights and Global Justice, observed that the introduction of Digital Identity is affecting the political settlement or social contract between governments and their citizens. In her session ***The shifting burdens of digital identities in public service delivery: Implications for human rights, social inclusion, and trust***, Cioffi shared experience, over two decades, of senior citizens' rights to access payments in Uganda, noting the impact on authority, accountability and ultimately levels of exclusion. She also discussed the parallels with the integration of digital ID and public services in several other countries, including the use of India's Aadhaar system, and the United Kingdom's Universal Credit and Verify UK.

"You can see in the case studies that the introduction of digital ID allows the government to remove authority away from the community towards a centralised, different form of authority," she said.

As systems introduce many new, unfamiliar steps for individuals, and challenges for people living with poor internet connectivity, she said: "there is a transfer of burdens that fundamentally alters the way the right is realised. It is not just about the registration process; it is about additional barriers put in every step along the way and how that transforms the relationship between the individual and the state."

Over time, this transformed relationship is characterised by "a fragmentation of accountability across different public and private institutions," with the shift of administrative burden to individuals preventing the visibility needed to recognise requirements for adequate governance frameworks for the delivery of social security or health programmes. "What it is doing is increasing the contingency of rights," she said, adding that in the process: "Digital identity systems have the potential to harden and exacerbate existing inequalities."

Politics trumps everything

The impact of systems or service governance on citizen relationships, particularly when they are developed for broad public service requirements was echoed across many other case studies explored on the day. Babatunde Okunoye, Research Affiliate, Berkman Klein Centre for Internet and Society, Harvard University at the University of Johannesburg, described how a changing political climate in Nigeria seemed to threaten the future of the country's ID project 16 years after it was established.

His session ***Mistrust of government in context of repressive states as a driver of slow acceptance of digital IDs*** described "a brick wall of public mistrust" that emerged as people became aware of the levels of central control facilitated by an identity system. Nigeria's programme, often celebrated as a success with 56 million people enrolled, had not seen any major public pushback until the government introduced a policy requiring people to link their national identity numbers (NIN) numbers with their SIM cards and later their IMEI (device registration) numbers. The move coincided with the Autumn 2020 #EndSARS[1] protests in which many lost their lives, and others found themselves on police surveillance lists.

"People said no. That is enough. You cannot have my international mobile identity equipment numbers (IMEI). I will not link my SIM to my name. The distrust was so strong that the deadline had to be moved seven times because people just refused."

Okunoye noted that people become aware of the levels of central control facilitated by NIM as it links biometric and other identity data together with many other datasets such as passport, banking, health insurance, pension, drivers' license, and more. He highlighted a need to account for inherent "administrative curiosity" that motivates the development of systems that facilitate "comprehensive knowledge of the governed," and challenged the trend toward centralised digital identity systems that are occurring within many African nations.

Citing prevalence of fledgling democracies on the continent, while also noting the rejection of centrally run ID programmes or the linking of government datasets in the more established democracies of the United States and United Kingdom, he stated: "... as someone who lives in the Global South, someone who has worked here and also works in civil society, what is bad for the US and UK cannot be good for us. Because of our contexts, these systems are more prone to abuse."

"Politics trumps everything. The nature of government in power can make a nonsense of whatever design is implicit in particular ID systems.... We spoke a lot already about what is happening in Afghanistan with the government who left precious data at the hands of the Taliban. What was used as a tool for management became a hit list. You might have an okay government now, but you don't know what they will be like ten years from now."

Assessing the Data Protection Assessment

Another session, ***The Digitisation of the Brazilian National Identity System*** also put a particular focus on accountability measures. Concerns highlighted the linking of civil, electoral, judicial and criminal databases using biometric data to identify everyone, and the pressures from the COVID-19 Pandemic that are driving significant growth in the digitisation of public services. Established in 2017, three years in advance of the country's data protection legislation coming into force, the identity system has evolved rapidly within the context of a new digital government strategy and supporting digital government law which came into force in March 2021.

"Brazil does not yet have a strong data protection culture, so it is something we want to highlight," said Marina Meira, Project lead, Data Privacy Brazil Research Association.

"One interesting point we are saying is that the government is not a simple entity. You cannot be a small city requesting any information about a citizen from another city that has no pertinence to your job. Why are you requesting it? It has to have a procedure (to determine) why you would want it?."

Drawing on findings from their advocacy work and a study funded by the Open Society Foundation on the prevalence of data protection impact assessments that have accompanied the introduction of IDs, researchers described the country's national data

1 October 2020 protests against the eventually-disbanded police unit, the Special Anti-Robbery Squad (Sars) and greater calls for better governance of data and surveillance by protesters after protester shootings took place by men in army uniform.

protection authority as fragile. As a new ministry, it was short staffed and had ties to the presidency of the Republic which nominated its directors. By contrast, the gov.br website and mobile app created as a centralised portal to all branches of government, has been well resourced. The system introduced new approaches for public service delivery, including pilots of liveness testing using facial recognition technology that queried the national identity database to satisfy a requirement for retired people to prove they are alive and could continue to receive pensions.

"Currently, more than 70% of government services are already digital or partially digital, and there are more than 110 million users – more than half of the Brazilian population" said Marina Garotte, Researcher, Data Privacy Brazil Research which is also participating in the study. "500,000 (half the people eligible) were invited to take part in the 'pilot' initiative."

Regulate operational requirements

An overview of another long-established national identity system, ***Assessment of the National Integrated Identity Management System in Kenya,*** provided an opportunity to consider the comprehensive policy and legislative considerations to be anticipated. Victor Kabata, Post Doctoral Research Fellow, Sorbonne University, Abu Dhabi particularly emphasised the need to address operational requirements that back up governance and enforcement agencies, alongside laws to ensure the whole digital economy and space within a country can be trusted, for a digital ID system to operate effectively. Data protection, he suggested, must be constitutionally enshrined.

Citing Kenya's 20-year history with developing a digital national identity system, he highlighted the country's explicit reference to the right to privacy in it's constitution and data protection legislation implemented in 2019. Kenya is also a signatory to various international instruments guaranteeing the right to privacy, including the universal declaration of human rights.

Despite this, Kenya's broad-reaching ID system initially developed to close an identity gap[2] in the country and facilitate access to government services has suffered a lack of public confidence. "This is seen by the low rate of registration and the fact that of those who are registered, the majority have not even collected their identity cards."

"In Kenya's case, the oversight authority for the identity system or registration of persons act is very much reliant on the executive in terms of funding. The implementing body (a government Ministry) that has been mandated to implement this system is part of the executive. In the case that there are any data breaches, it becomes difficult to oversee or question these ministries."

Referring to the office of the data protection commissioner, he said that while it is independent on paper, practically "there is a lot of influence from the executive."

The defining influences

In understanding a way forward, the speakers pointed to the opportunity in accounting for the defining influences that led to the scenarios they had documented in their research.

"There are clearly ways in which the use of a digital identity system is actually being used as a reform of the welfare state under the guise of a performative and digitalisation agenda. After a while, it becomes about servicing the infrastructure," observed NYU's Cioffee. "We are seeing that in Uganda and other places, where the need to develop an identity system has led the government to try and coerce people to sign up through access to social rights, typically targeting those who are most vulnerable and historically excluded. It is because the infrastructure needs to be serviced and has become a policy part of its own, rather than being seen as a mechanism of improving service delivery, so you get that flipside of the policy priorities."

2 Reach that proportion of their population without any form of legally recognised ID.

Okunoye suggested a change in focus for the humanitarian-inspired efforts, including National-level foundational systems supported by the World Bank Group's effort to support the United Nation's sustainable development goal 16:9 to provide legal identity for all. "In Nigeria, the voters registration is 84 million people already. That is more than the (almost) 60 million for the current national identity project. What if the World Bank decided to fund upgrading the voters' registrar, operations registers and so forth so that it achieves the same aim of giving people some sort of identity to participate in national life[3]," he said adding, "I'm just worried that I saw a tweet one day that said because the World Bank is funding this, it is right and just. Not necessarily. In Africa, we are still building our institutions."

A lesson from neuroscience

"Expectations can be cultivated and created in a collaborative fashion. The trustee can play an active role in shaping the expectations. They can be open and honest, and they can also take steps to prevent situations where trust cannot be fulfilled," concluded Paul Smart, Senior Research Fellow, University of Southampton, who presented work that draws from understanding in neuroscience about how brains predict sensory inputs to model the implications for trustworthy systems design. His session, was titled ***Relativistic conceptions of trustworthiness, explained the challenges of projecting a human-to-human concept into systems.*** "There is surely a sense in which we want trustworthiness to be a property of the system. We want an absolute or simple sense of trustworthiness as opposed to a realistic one in which trustworthiness is relative to particular people," he said.

In considering the trustworthy state of systems, Smart's model ranks a number of problems related to our theoretical understanding of trustworthiness to determine the features that can be designed into systems to minimise them and produce the desired absolutist view.

Tensions between an absolutist conception of trustworthiness and a relativist concept are resolved through communication and negotiation aimed at managing the possibility of betrayal and minimising gaps between expected and actual outcomes. This puts an emphasis on the role of transparency, education and communication. "I think this helps to direct attention to the importance of individualised forms of control, consent and authorisation. This relates to the capacity of individual users being able to exert control over the operation of an identity system, such as restricting access to identity-related information."

3 In Q&As the speaker pointed out that many existing systems such as the electoral register are in a digital format

Trustworthy design thinking for systems and AI

"Technology must be seen in light of the societal problem that it seeks to address."

Fran Meissner, Assistant Professor, University of Twente.

Industry and sector-specific developments reveal a move toward decentralised systems, sometimes referred to as self-sovereign identity where verifiable credentials are held by the people (or entities) that interact with an organisation, rather than the organisation itself. Describing benefits for security and privacy, alongside better outcomes for customers, presenters examined new approaches that address challenges not just for identity systems but also the evolving business models they support.

The session ***Decentralised ID, verifiable credentials, zero trust represent a new paradigm for trust/ verification,*** highlighted that the internet was not designed to facilitate knowing who or what was connecting to whom. Speakers noted a desire to "limit the problems that we have in credentialling," as growing in significance for cyber security management with growing adoption of a cyber security strategy known as zero trust for private-sector and public services. Zero trust manages all, including employees as external system users and relies on an ability to verify expressly.

"We are seeing the adoption of travel and border management for COVID-19 testing, we see passwordless login an urgent thing to ensure our protection and we see rapid adoption of zero trust environments in this space," explained Dr Chase Cunningham, an author and chief strategy officer, Ericom software and Heather Dahl, CEO of Indicio.tech – a solution provider described as a public benefit company supporting the open source and interoperability goals of the decentralised identity community.

Citing statistics from North America that point to developing dependencies on online accounts, credit, and remote access to work ushered in with a 70% increase in remote connectivity, Dahl pointed to a recent decision by the Government of Ontario, Canada to invest in decentralised identity to allow people and businesses to identify who they are online. It aimed to generate economic advantages worth £20 billion. "What we see is that Ontario is leading a whole slew of government and business interest in decentralised identity systems. It would be interesting to follow who looks at the Ontario decision and decides to adopt a decentralised identity for their own infrastructures."

Advantages described included the flexibility to support varied organisational and operational requirements, while also minimising data collection and storage for an internet-dependent working and commerce space.

"Often we think about identity as something that is assigned to an individual but in the case of decentralised identity, it can be a thing, it can be a business. In the case of agriculture, livestock, animals... Anything out there, even a process or document

can have its own identity. In the near term IoT, smart city management is a perfect situation for verifiable credentials in sharing data between the devices," explained Dahl. "It might sound futuristic. It is actually not. Today there are products available for commercial implementation, there are secure open-source code bases to build upon. ...You can look at the governance behind that and see if it meets the requirements of your acceptance."

Facilitating transition

The session, ***The role of digital identity in mortgage eligibility decisions,*** provided an example of how a decentralised approach to identity could transform how people apply for a mortgage but there is a need to accommodate the dynamics of a transition to such a system. "The key barrier to adoption is adoption," explained Edward Curran, Knowledge Transfer Partnership Associate and Systems Engineer with Newcastle University, who presented collaborative work underway with Durham University, Atom Bank and Innovate UK. "Nobody wants to make the first move.[4] It is kind of a tricky situation. We want to break the deadlock. We have gathered some requirements for going on this journey of what we want our system to be able to do."

The work deploys two sets of open standards: WC3 verifiable credentials to store a generalised version of identity and mortgage application data within a digital wallet, and DMN, for logic automation to allow borrowers to make multiple, simultaneous applications to different lenders. Creating an opportunity to reduce application effort and cost for both lenders and borrowers, the overriding aim is to help borrowers gain the confidence to seek better deals.

Citing a 2019 mortgages market study published by the UK Financial Conduct Authority which concluded that 30% of cautious users have missed out on getting a better mortgage due to fear of rejection, Curran advocated that: "It should be easy to access trusted data, as desired by the verifier so they should have flexibility to find what they consider trusting in their own time."

The proposals and systems specifications being outlined build on the start given with open banking standards to standardise schemas and allow for more portability of customer data to reform a process that currently requires similar credentials to be repeatedly submitted to different lenders. Designs are based on a user-controlled interface that accommodates both the use of digital wallets, and API - based services and allows for the execution of domain expert led "trusted inferences."

"We have a user interface which presents the schema of the (verifiable) claims which are available, visually, and then you (the lender) can select which claims are required," he explained. "The practical requirement is to be able to fulfil common interfaces needed of the industry now, rather than just in the future, but we also want to support the kind of better models of identity which we hope will occur."

Relevant intelligence

Given the scale, varied areas of complexity, from the analysis of biometric data to the verification of claims, and the volumes of data involved, artificial intelligence (AI) is increasingly deployed within identity systems. Research interest on this development at the conference touched on opportunities to both manage varied risks and, in creating systems that are more representative, deliver services that are more effective.

The session ***Intersectional approaches to data can inform the development of trustworthy digital identity systems,*** was presented by a team from the UK's University of Sheffield. They set out their efforts to look across the data value chain for opportunities to enhance the algorithms at the heart of creating the artificial intelligence of a given system.

"Our research uses data from an intersectional perspective, an idea that has grown from Black feminist thought. It is commonly known as a critical framework to understand how multiple aspects, such as age, gender and ethnicity come together in a time

4 The benefit is seen to be with the consumer until the market shifts

and place, to increase privilege or discrimination, or disadvantage or advantage that a person experiences," said Chisenga Muyoya, Research Associate, University of Sheffield, while emphasising that intersectionality is a theory and a practice. "It's not enough to design an effective system, without considering the risk, holistically, for the most marginalised in a context as well as over time."

Advancing a concept of institutional trust, using an intersectional framework, reminds organisations that they have to build an evidence base around how well the system is actually benefiting people. "We are interested particularly in the perspectives of the most marginalised in society," outlined Caitlin Bentley, Lecturer in AI-enabled Information Systems, University of Sheffield. "Our focus in this research is really on developing context where a lot of these (data management) systems don't exist. A lot of these countries that we are thinking about here lack the data systems around health, around statistics, around all sorts of things. We are looking at those interactions where people have direct interactions with digital ID systems, but also how the systems are impacting on their lives and their outcomes, their personal outcomes. Getting a job or accessing health, things like that.

"There are already communities, as well as civil society organisations, that are working in these areas, that are handling enormous amounts of data. They do need better support to give a voice to institutions that also may not have the necessary competencies to handle this information" concluded Bentley.

A public view on biometrics

"New disputes around the use of biometric ID systems are cropping up all the time, and as these feature and become more visible and common, these challenges are only likely to become worse," said the Ada Lovelace Institute's Harry Farmer, who presented the results of their Citizens Biometrics Council in the session ***Biometrics for identification – What do practitioners need, and what can government do?*** Conclusions drawn from the exercise conducted in the United Kingdom over the course of 2020 led to a call for specific regulatory governance in not of biometric technologies within identity and broader applications.

Farmer said: "the public are actually pretty aware of the ability of biometric identification tools and technologies to be used to undermine privacy. They are sensitive to the fact that biometric ID systems that can enable ambient surveillance that is difficult to become aware of and quite difficult to escape, and they are aware of the potential of that kind of surveillance to undermine free, open societies."

The speakers also noted that consent to the collection of biometric data required a level of transparency that is tricky to achieve: "If doing something you need to do is dependent on being subject to biometric processing, then you cannot be said to have consented to it," explained Farmer.

Findings demonstrated that these systems are contributing to marginalisation as they continue have differential rates of accuracy for particular groups, with deep concerns particularly for failing trans and disabled people.

"A lot of suggestions were around lowering stakes for failure and error. There was talk around the need to have humans in the loop so that errors could be flagged and contested ... a general feeling amongst the public that there should not be the use of biometric identification systems for anything where failure (the delivery of an inaccurate conclusion or no conclusion) would be catastrophic. They talked a lot about proportionality and questions of when to use biometrics. The response clearly from them was: don't use a biometric system when another form of identification or when another solution will do," Farmer said, adding that the concept of proportionality extended to the storage of biometrics. Farmer said, "the view was, don't hold onto more data than you need for longer than you need to and don't share it unless absolutely unavoidable."

AI and border control

As the use of biometrics for border control grows, researchers from University of Twente, in the Netherlands asked the question: ***Can border AI be trustworthy for migrants?*** to both look for opportunities to develop richer context, and examine drawbacks that may overshadow the seamless nature of moving through borders using a part of your body. Their first observation was that the use of biometric identity in a politicised application such as the control of migration at borders, is quite different from what people might think about in other contexts.

"Technology must be seen in light of the societal problem that it seeks to address. In the migration literature we have very little consensus on how exactly migration ought to be regulated or what exactly ought to be some markers of individuals that would be siphoned out as being potentially dangerous or making fraudulent claims. We have a context that is potentially one of life and death stakes. Further, these are things are changing continuously, so it might not be possible to write criteria for clearing into a system, " said Fran Meissner, Assistant Professor, University of Twente. as she pointed out that such criteria "might become non-negotiable when they are actually integrated into systems which assume a kind of predictive ability of migration movements which simply in empirical terms we have not yet been able to witness."

The team is exploring the use of a guidance ethics approach for designing border AI that is shaped by dialogue taking into account not just human features, but also a richer profile of migrant populations and criteria for human safety. Systems that can consider biometric traits alongside behavioural traits may be able to identify the most disadvantaged, while facilitating other relevant considerations. "I would be interested in understanding to what extent the mistrust in migrants as a baseline can be reshaped to allow room for migrants to really negotiate or change the perception about their livelihoods and about their profile and potentiality. In our view, this might be meaningful not only for those hosting countries and those hosting authorities who decide about them but also would allow for room for migrants to show their human vulnerabilities," said Karolina La Fors, Post-doc in Responsible Design, DesignLab, University of Twente.

La Fors also pointed out that such an approach fills gaps left by current legislative guidance, including Europe's wide-reaching GDPR and the European Artificial Intelligence Act, which were characterised as very systems focussed and having a lack of definition around proportionality and safeguards against human rights abuses. "When we look at the formulation, we can manifest that this is rather about the safety of the system, rather than about the safety of potential data subjects. .... the risk assessment regarding these technologies are again highly technical and only indirectly focusing on the livelihoods of migrants."

Thoughts for the future

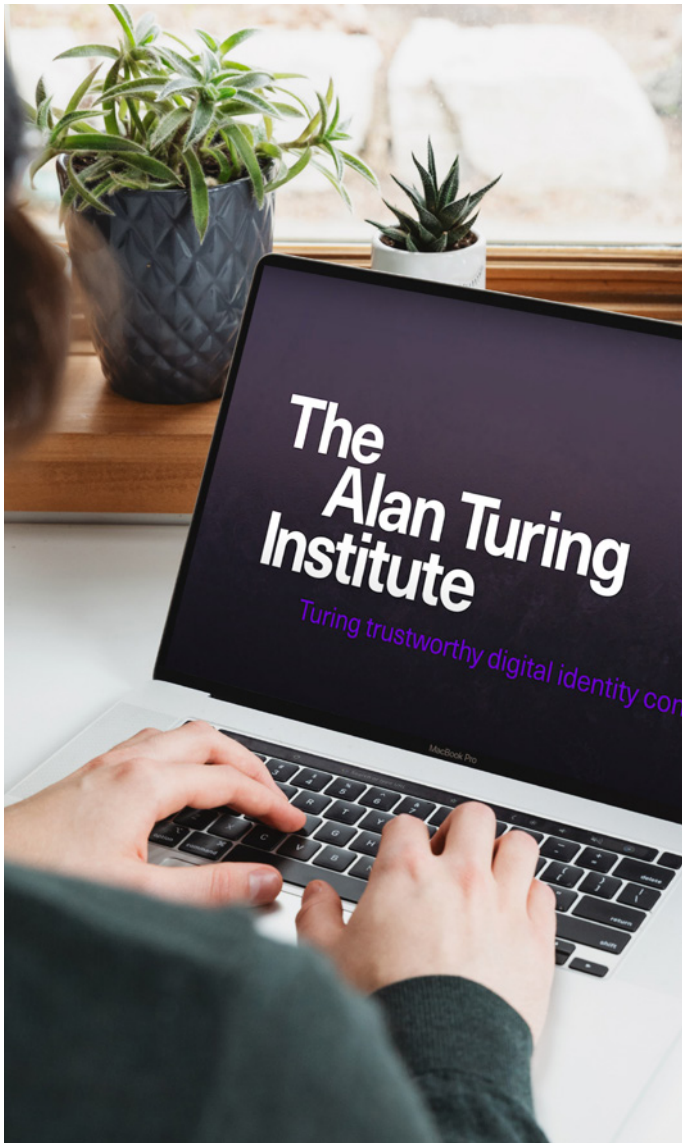
Considerations for the advancement of Trustworthy Digital Identity systems are growing in importance as these systems become the gateway to opportunities and resources in modern society. Our first conference dedicated to the subject provides clear testament to the rich body of research working to enhance understanding of their impact and the maturity needed to achieve projected goals. This research is not just the purview of academia but takes on many forms with industry, associations, NGO's and humanitarian organisations bringing insightful contributions to the conversation.

While we were only able to dive into a few examples on the day, the event surfaced a breadth of considerations that give us all pause for thought. They challenged current practice including the repeated collection of similar data; the linking of datasets across multiple government departments; the growing application of biometrics in commercial and public-service scenarios; the reliability of algorithms and even the necessity of establishing purpose-built national systems rather than enhancing existing ones to facilitate access to national life. They emphasised an imperative to look beyond data protection and systems security requirements to anticipate, manage and robustly regulate the many risks we are only beginning to appreciate through the lived experience of digital identity implementations. There were also many opportunities advanced for improving outcomes for customers, migrating populations, and other pockets of society.

Almost all pointed to a detailed focus on what a system is supposed to achieve over the broad application of technology, or collection of data within a generic system—and the room to determine how or whether technology should facilitate it.

The full playlist of conference presentations is available on The Alan Turing Institute YouTube Channel.

Find out more:
Sign up for the Trustworthy Digital Identity Newsletter
Join our Trustworthy Digital Identity interest group



The poster galleries

The following conference posters summarise information or research concisely related to the themes of the Trustworthy Digital Identity Conference. They were presented in an online, booth style gallery and invited offline discussion with the authors of the posters to further consider research areas of mutual interest.

Dynamic cyber risk estimation with Competitive Quantile Autoregression

By Raisa Dzhamtyrova and Carsten Maple

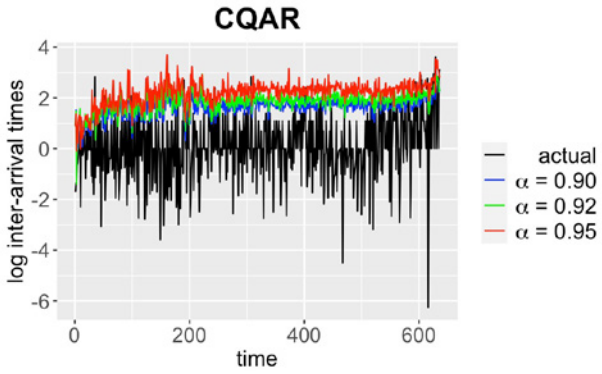
Outcomes

- A new analysis and adaptation of Quantile Autoregression (QAR) for calculating cyber Value-at-Risk (VaR).
- A new dynamic risk estimation method, Competitive Quantile Autoregression (CQAR), with a theoretical guarantee on its performance.
- We show that both QAR and CQAR can be used to estimate VaR of cyber breaches' sizes and inter-arrival times.

Modelling of hacking breaches

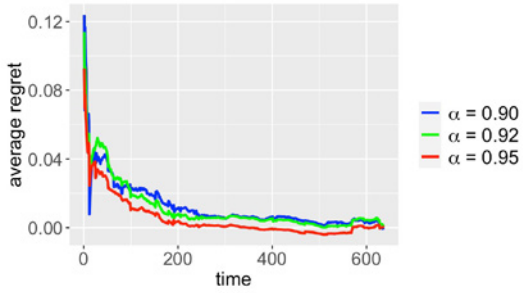
We use the Privacy Rights Clearinghouse report, which contains the chronology of the data breaches since January 2005.

It is important to estimate how large the potential losses might be in order to prevent or hedge losses. VaR is modelled with high significance levels.



Theoretical bounds

An important property of CQAR is that it asymptotically predicts as well as the best QAR, i.e. average regret between cumulative losses of CQAR and QAR goes to zero as time increases.



Links

https://arxiv.org/abs/2101.10893

https://github.com/alan-turing-institute/dynamic_cyber_risk

Contact

Raisa Dzhamtyrova

The Alan Turing Institute

rdzhamtyrova@turing.ac.uk

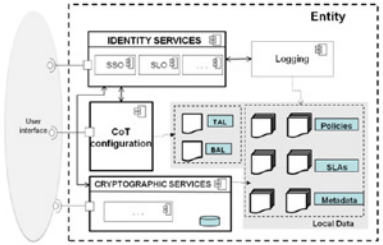
A Comparative Cyber Risk Analysis between FDIM and SSI

By Anh Tuan Le, Gregory Epiphaniou, Carsten Maple, Al Tariq Sheik, Ugur Ilker Atmaca

Outcomes

This work provides **attack surface analyses** for the **Federated Identity Management** (FIDM) and the **Self-Sovereign Identity** (SSI) management systems in order to develop a reference for the comparison of security and privacy risks between the two systems. Firstly, the **threat landscapes** of each system were comprehensively synthesised from their main components and functionalities. Secondly, this work offers **a use case analysis** that employs the attack surface analysis to compare the cyber-risks of the two systems in detail when **managing healthcare records.**

FDIM General Architecture



Circle of Trust (CoT) Configuration

Identity Services include Identity Providers and Relying Parties

Cryptographic Services

Logging

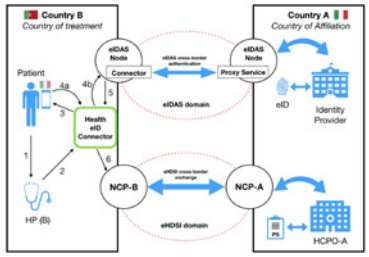
Data Storage

FDIM Security Analysis

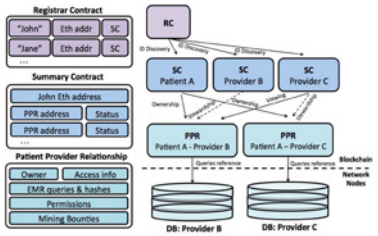
COMPONENTS	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23
User access right	■	■	■	■	■	■																	
Components							■	■	■	■	■	■					■	■	■		■	■	■
User information																	■	■	■		■	■	■
Relying Party		■	■	■	■			■	■	■	■	■					■	■	■				
Identity Provider						■							■	■	■	■	■	■	■				
Logging	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■
Storage													■	■	■	■	■	■		■	■	■	■

A1. Code/Token/State leak attack
A2. Token spoofing
A3. Replay of authorisation code
A4. Manufacturing fake token
A5. XSS attack
A6. Third-Party Resources Attacks (Malware)
A7. Redirect Attack (307 redirect)
A8. Naive RP Session Integrity Attack
A9. Flow interception
A10. Session handling
A11. Injection attack
A12. Man in the middle Attack
A13. IdP Mix-up attack
A14. CSRF Attacks and Third-Party Login Initiation
A15. Server-Side Request Forgery (SSRF)
A16. IdP account compromise
A17. Snooping
A18. Network Eavesdropping Attack
A19. DoS Attack
A20. Elevation of Privileges Attack
A21. PII leakage
A22. User Profiling
A23. Location Tracking

Use Case: e-Health Identity Management



FDIM: eIDAS over openNCP (Burrai, 2019)



SSI: MedRec (Azaria et. al., 2019)

Risk Analysis Comparison

Criteria	FDIM: eIDAS over openNCP			SSI: MedRec		
	Likelihood	Impact	Risk	Likelihood	Impact	Risk
Consistency	L	H	M	L	L	L
Integrity	M	H	M	L	H	M
Authenticity	H	M	M	L	M	L
Availability	H	H	H	L	L	L
Confidentiality	H	M	M	L	M	L
Anonymity	H	H	H	L	L	L
Patient-control	H	H	H	L	L	L
Access-control	H	H	H	L	L	L

Use Case Comments

Security threats on the SSI systems tend to have lower likelihood and impacts compared to those of FIDM, but the FIDM vulnerabilities can be fixed faster.

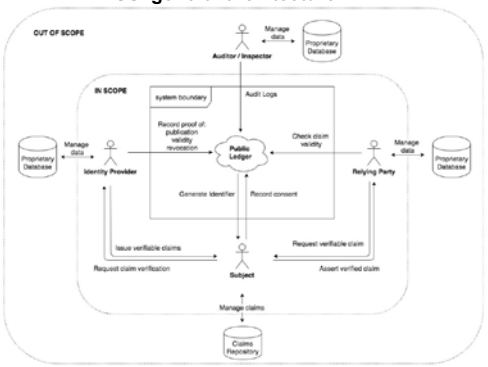
SSI systems have much lower risks of privacy leakages compared with the FIDM systems.

SSI Security Analysis

COMPONENTS	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11
Decentralised ID								■	■	■	
DDO								■	■	■	
DID Subject	■	■	■	■	■	■	■	■			■
Wallet Software	■	■	■	■	■	■	■	■			■
Microledger	■	■	■	■	■	■	■	■			■
Edge Agent	■	■	■	■	■	■	■	■			■
Universal Resolver									■	■	
Verification Data Registries									■	■	

B1. Key exposure
B2. Man-in-the-Middle (MitM)
B3. Reverse Engineering
B4. Wallet Query Language (WQL) Injection
B5. DID Wallet Database Information Disclosure
B6. Elevation Of Privileges
B7. Jailbreak/Rooting
B8. Phishing/Impersonation
B9. Cache poisoning/pollution
B10. VDR Partitioning
B11. Social Recovery Attack

SSI general architecture



Contact

Anhtuan Le

a.le.1@warwick.ac.uk

WMG

University of Warwick

Principles of Trustworthiness for Digital Identity Systems

By Nagananda, K. G., Maple, C. and Epiphaniou, G.

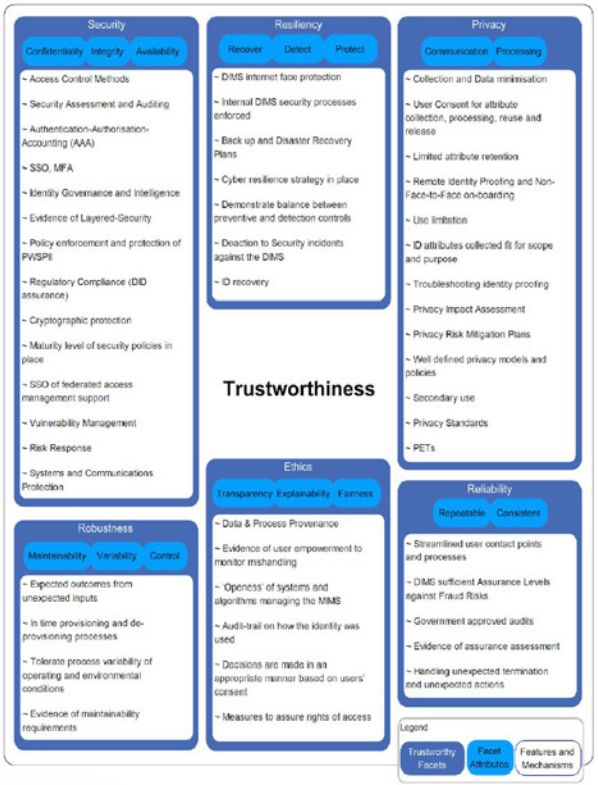
Outcomes

- We identify 6 different pillars of trustworthiness in the context of Electronic Identity Management Systems (EIDMS): security, resiliency, privacy, reliability, ethics & robustness.
- Provides a holistic understanding of the perceived versus achieved trustworthiness for EIDMS.

Background

- EIDMS is a critical infrastructure for digital economic activities: ID verification & proofing, financial transactions, etc.
- Understanding the different trust & security requirements is, therefore, important.

Pillars and attributes of rustworthiness



Main objectives

- Identify metrics and measurement mechanisms for each of the pillars.
- Define trustworthiness assurance levels (TALs) based on the metrics.
- Compare different digital identity systems using TALs.

Contact

Nagananda, K. G.

The Alan Turing Institute.

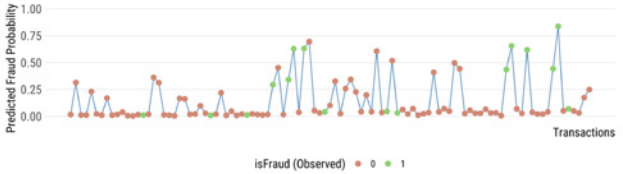
ngurukumar@turing.ac.uk

A fusion model for fraud detection

By Santhosh Narayanan, Mark Briers, Mark Hooper, Carsten Maple

Outcomes

- Most machine learning algorithms are agnostic to the natural ordering of events over time.
- Point processes, however, can model temporal dynamics like clustering and dependence on past occurrences.
- Extending marked point processes into a classification model is novel.
- Fusing point processes with conventional ML classifiers can overcome limitations and offer better predictive performance.
- The point process model also offers insights, for e.g. that fraudulent events are triggered almost exclusively by past fraudulent events.



Dataset

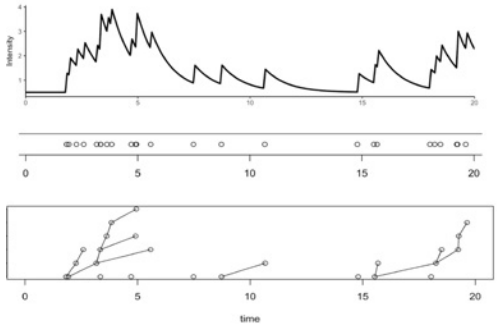
From the Kaggle competition,

IEEE-CIS Fraud Detection: Can you detect fraud from customer transactions?
https://www.kaggle.com/c/ieee-fraud-detection

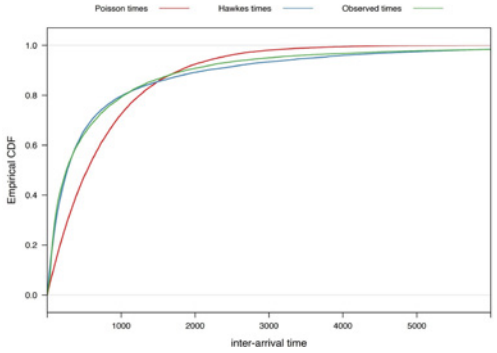
Contains over a million real-world e-commerce transactions with fraud labels.

Hawkes processes

A self-exciting point process model that captures clustering of events as well as dependence between different types of events.



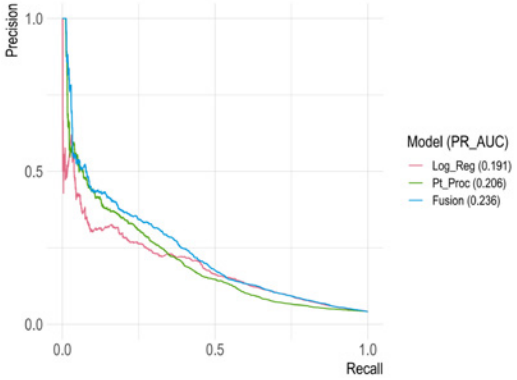
The Hawkes conditional intensity function and branching structure of the process showing the triggering of events.



CDFs from a Poisson process, a Hawkes process and the observed times of fraudulent events. Hawkes is a good fit confirming that fraudulent events cluster in time.

Validation

- Using area under the Precision-Recall curve as predictive performance on the positive class (fraud) is more important.
- Model fusion by averaging predictions from a logistic regression model and the point process based model.
- Using only the occurrence times and no other covariates, the point process model outperforms logistic regression, proving the value of modelling the temporal dynamics of such data.



Contact

Dr Santhosh Narayanan
snarayanan@turing.ac.uk

Audience contributions

"I think that we do need to assume that there is no specific trusted actor, we have to elicit out what could go wrong and then by bringing threat and risk assessments we can say what is the likelihood of something like this happening?"

"Just a quick note to say that yesterday was marvellous. It's a long time since I attended an Identity conference where I learnt so much – brilliant to hear from such a diverse group of presenters and such a professional job from you and the team at the Turing."

"Turing at its best - a challenging subject, all angles covered. Enjoyed on-line chat!"

"Thank you! Great conference , ... especially around privacy-enhancing biometric tokenization - which could have prevented a lot of the issues."

Trustworthy digital identity at the Turing

As many approaches to ID systems evolve at pace, increasingly with the influence of governments, the world is learning with these developments about their impact, their potential and the risks as the incentives to misuse, commit fraud, breach or manipulate these systems grow with their scope. We have a real challenge before us to enhance understanding of how these risks, and of course the underlying vulnerabilities are changing; and a real opportunity to design systems and processes fit to manage them.

The Alan Turing Institute Trustworthy Digital Identity conference is part of a set of initiatives to bring together and work with the global community of stakeholders interested in pursuing this opportunity. It complements a significant research project on Trustworthy Infrastructure for Identity Systems launched in 2020 with initial grant funding from the Bill & Melinda Gates Foundation. 18 months into its 4-year mandate, a community of over 35 researchers have allowed us to drive understanding of emerging risks, requirements for assuring trustworthy outcomes, and varied interventions with prototypes and technical briefings made openly available through the project web pages, or GitHub, where they can be regularly scrutinised.

Papers developed to date document the evolving risk landscape, dive into developments with facial recognition, and also explore opportunities for risk modelling and governance, novel privacy-enhancing protocols for data management, and verification opportunities using the feature phones that are more widely accessible than smart phones in developing economies. The project is also advancing a Trustworthy Digital Identity Systems Framework, which defines six facets of trustworthiness as a key resource for the project and global community of systems implementors.

The research is complemented and informed by the efforts of a Trustworthy Digital Identity Interest group at the Turing. Launched in December 2020, the group has about 100 members and meets monthly to share experience and elevate key questions, bringing together a unique cross-section of academia, standards, public sector-practitioners, technical and industry contributors.

This document was prepared by Lyndsay Turley based on the presentations given at the **Trustworthy Digital Identity Conference**, 2021.

Follow the progress **#trustworthyid**
turing.ac.uk/research/research-projects/trustworthy-digital-infrastructure-identity-systems

Twitter **@turinginst**
LinkedIn **school/the-alan-turing-institute/**
Sign up to the newsletter: **turing.ac.uk/contact-us/join-our-mailing-lists**