# Software Tools for Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reduce human-relaTed risks

Tasmina Islam and Shujun Li
School of Computing, University of Kent

## Introduction

The focus on cybersecurity as a dynamic interaction between humans and socio-technic elements within a risk ecosystem raises practical issues of implementation and conventionally these issues are often considered under 'raising awareness'. Key to make these awareness activities more effective in influencing human behaviour is to properly incentivise people, businesses and organisations to participate and adapt their behaviour. But due to lack of information about *dynamically evolving* personal preferences (which need collecting dynamically and at individual level) these may still not be effective. While there is isolated research across these areas, there is no holistic framework combining all these theoretical concepts (co-evolution, opportunity management, behavioural and business models, ad hoc technological research on cyber risks and specific types of cybercrime) to allow a more comprehensive understanding of human-related risks within cybersecurity ecosystems and to design more effective approaches for engaging individuals and organisations in the reduction of such risks. Filling this research gap is the aim of this proposed project.

## Software Development Objective

A series of software tools is being developed for active engagement of users in cybersecurity ecosystems, including data management for data sharing (collection), user and community profiling based on shared data, cybersecurity risk evaluation and personalised/ contextualised communications (including risk visualisation tools). Our goal is not to develop such tools from scratch, but base them on mature technologies and software which we will integrate into a user-friendly toolset for each user group and also investigate behavioural models to allow us to incentivise individuals to engage

> Behavioural Sensing + Lightweight Configuration
> + Personalisation + Contextualisation + Server-side AI
> ⇒More User-friendly Reporting

> Personalisation + Contextualisation + Ontology
> + Hybrid Human-Machine Computing
> + Behavioural Nudging + Closed Loop
> ⇒More Effective Awareness/Crime Prevention Campaign?

## Main Aspects

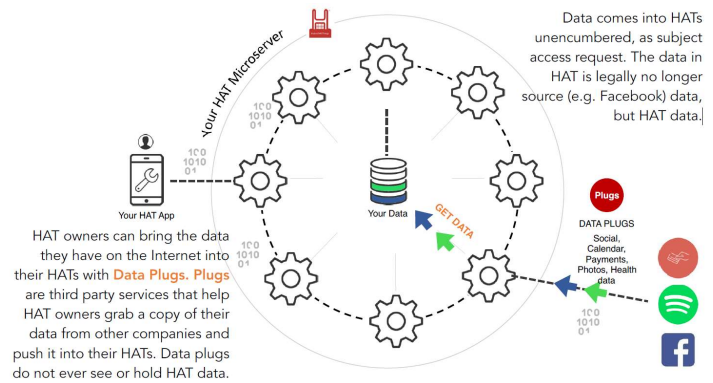Two main aspects of the software development:

> Human related location privacy and behavioural model analysis
> ⇒ System reporting risks to human
>
> # A mobile app
> # Based on Hub of All Things (HAT)
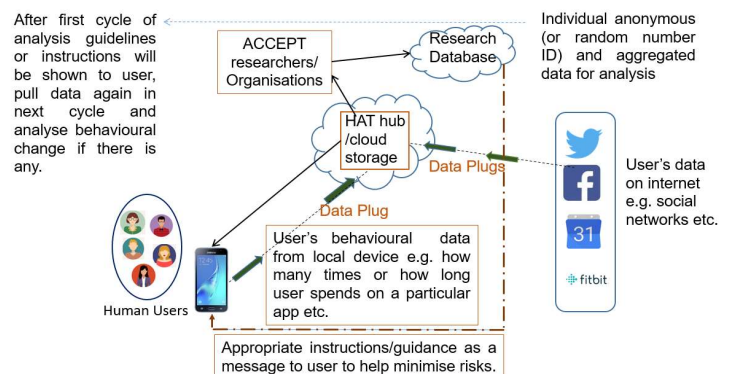> https://www.hubofallthings.com/

> Human as a Security Sensor (HaaSS)
> ⇒ Human reporting to system with feedback loop
>
> # An Windows app
> #Based on CogniSense

## HAT Infrastructure



Data comes into HATs unencumbered, as subject access request. The data in HAT is legally no longer source (e.g. Facebook) data, but HAT data.

HAT owners can bring the data they have on the Internet into their HATs with **Data Plugs. Plugs** are third party services that help HAT owners grab a copy of their data from other companies and push it into their HATs. Data plugs do not ever see or hold HAT data.

DATA PLUGS
Social, Calendar, Payments, Photos, Health data

## Mobile App Framework



After first cycle of analysis guidelines or instructions will be shown to user, pull data again in next cycle and analyse behavioural change if there is any.

Individual anonymous (or random number ID) and aggregated data for analysis

User's data on internet e.g. social networks etc.

User's behavioural data from local device e.g. how many times or how long user spends on a particular app etc.

Appropriate instructions/guidance as a message to user to help minimise risks.

## The CogniSense HaaSS Feedback Loop