An Exploratory Analysis of the Security Risks of the Internet of Things in Finance

Carlton Shepherd[1], Fabien A. P. Petitcolas[2], Raja Naeem Akram[1], and Konstantinos Markantonakis[1]

[1] Information Security Group, Royal Holloway, University of London, Surrey, UK, {carlton.shepherd.2014, r.n.akram, k.markantonakis}@rhul.ac.uk,
[2] Vasco Data Security, Wemmel, Belgium

Abstract. The Internet of Things (IoT) is projected to significantly impact consumer finance, through greater customer personalisation, more frictionless payments, and novel pricing schemes. The lack of deployed applications, however, renders it difficult to evaluate potential security risks, which is further complicated by the presence of novel, IoT-specific risks absent in conventional systems. In this work, we present two-part study that uses scenario planning to evaluate emerging risks of IoT in a variety of financial products and services, using ISO/IEC 20005:2008 to assess those risks from related work. Over 1,400 risks were evaluated from a risk assessment with 7 security professionals within the financial industry, which was contrasted with an external survey of 40 professionals within academia and industry. From this, we draw a range of insights to advise future IoT research and decision-making regarding potentially under-appreciated risks. To our knowledge, we provide the first empirical investigation for which threats, vulnerabilities, asset classes and, ultimately, risks may take precedence in this domain.

Keywords: Internet of Things, risk assessment, finance, security

1 Introduction

The Internet of Things (IoT) – the notion that everyday objects will act on the environment and gain Internet connectivity – is projected to transform various sectors, such as agriculture [24], logistics [11], manufacturing [32] and healthcare [35]. The vision that IoT will be adopted into most business processes necessitates the development of technologies to secure it. Managing potentially sensitive data from an unprecedented number of sources, malware, and designing infrastructures with hugely heterogeneous devices are widely-recognised security challenges [38].

IoT is projected to significantly impact the financial sector in particular [13]. The abundance of business- and consumer-held IoT devices – whether in the home, on business premises, or held personally – may enable novel payment methods, finer customer profiling and more accurate pricing of financial products. The concept of pricing insurance from sensing devices, e.g., for home [27]

and life [8] products, is long-standing. Vehicle telematics have, most notably, been deployed widely for pricing motor insurance premiums more accurately from driving style [28,35]. Enterprise analysis products, like IBM's Watson IoT for Insurance [16], are becoming deployed for computing insurance risks at scale from customer IoT data. Salesforce IoT Cloud [29], similarly, aggregates customers' IoT data – behavioural and contextual information from personal devices – for user profiling. Additionally, IoT devices have been targeted for interacting with financial data more conveniently, e.g., stock tickers and trading platforms for smartwatches [14]; building energy budgeting models using ambient data from the home [5]; and conditioning smart contracts using in-transit environmental data [12]. Tata Consultancy predicts that, by 2018, over $207m will spent by financial firms on IoT-related product development [33].

Despite the growing number of applications, however, little academic work exists to assess the risks it poses to users and providers. In insurance, malicious customers may offer fraudulent data to providers to falsely achieve cheaper premiums. Alternatively, the value and volume of data produced by IoT devices may complicate customer data protection, potentially exposing businesses to significant reputational and legal risks. In this work, we address this space by methodically quantifying the risks involved with plausible IoT financial situations, using scenario planning scenarios and ISO/IEC 27005:2008 [1]. We examine a cross-section of consumer-centric financial products and services, such as insurance, in-branch banking and frictionless payments, to formulate scenarios in which IoT could be applied. The risks are evaluated using a detailed internal risk assessment with 7 financial security professionals with 55 combined years experience, before comparing them with a survey with 40 external security professionals in industry and academia. The contributions of this paper are as follows:

- Systemically quantifying the potential risks of IoT on a range of financial products and services, across a range of situations, with the assistance of scenario planning and ISO/IEC 27005:2008. To our knowledge, this is the first work that methodically grounds the potential risks of IoT in finance.
- Categorising and ranking these risks and a comparative analysis with existing opinions on IoT security from 40 security professionals.
- Recommended areas of focus, based on empirical analysis, for where IoT may impact most significantly in finance.

2 Related Work

While little work has been conducted on IoT in finance, academic risk assessments have been published in related domains, namely in mobile [34,20] and cloud computing literature [30], and RFID/NFC in air travel [2]. Theoharidou et al. [34] present a smartphone-based risk assessment methodology to address the shortcomings of traditional assessments (which typically consider smartphones as a single entity). Smartphone-specific assets – device hardware, operating systems and mobile applications of varying classes, e.g., finance and transport –

are used alongside application permissions and threat likelihood to derive risk values. The authors illustrate the methodology using an Android-based device and a test user with a managerial position in the pharmaceutical industry. The resulting risk values are intended to be incorporated with a regular ISO/IEC 27005:2008 assessment.

In healthcare, Lewis et al. [20] propose a methodology for assessing the risk of mobile applications by professionals, such as drug-dose calculators, reference and educational resources, and stored patient records. The authors focus on applications that may violate patient rights, e.g., health data remaining confidential and integral, and applications that may bring harm to parents. Healthcare-specific threats are incorporated in the risk analysis, e.g., whether clinical harm is reversible, in addition to typical threats, e.g., the loss of patient data. Such threats are subsequently paired with their associated vulnerabilities, e.g., absence of rigorous fail-safes and data encryption. These are combined with the physical capability of the application, such as a BMI calculator (low capability) or drug control device (high capability), to evaluate whether the application ought to undergo formal regulatory approval.

Saripalli et al. [30] propose the QUIRC framework for evaluating the security risks of cloud computing platforms. The work defines an impact factor, the effect of a security event on an organisation's assets and operations, and the probability of that event occurring to derive a risk value. An event's impact factor is drawn from its effect on six attributes – confidentiality, integrity, availability, trust, accountability and usability – and combined using a weighted sum as function of its probability. Event probability is determined from known statistics, such as the number of XSS and SQL injection attack reports. The authors also present a list of cloud and web security threats relevant to a QUIRC-based assessment.

Distinctively, our work assesses the risks of IoT in consumer-centric finance using technologies gaining traction in emerging academic and industrial research, e.g., car-based commerce [4] and smart contracts [12], as well as more mature technologies, e.g., vehicle telematics. The European Network and Information Security Agency (ENISA) conducted similar work in forecasting the risks of RFID on air travel [2,3]. Scenario planning – discussed in Section 4 – is used to examine these from a variety of demographics and applications, such as using programmable RFID tags placed in luggage to track whereabouts and to expedite check-in and boarding. Three scenarios are constructed in total covering a variety of such situations. The threats, vulnerabilities and assets involved in these are used to calculate risks using ISO 27005:2008, and a range of research and policy recommendations are proposed.

3 High-Level Methodology

Based on existing work by ENISA [2,3], we opted for a scenario-based methodology to plan IoT applications in consumer finance. Scenario planning is used routinely in the military [18], corporate planning [6] and governmental policy making [7,9,36] to evaluate emerging risks of plausible, but not yet realised, sce-

narios. Schoemaker describes scenario planning as the telling of realistic stories about plausible future events based on extrapolation from present trends, and *"helps expand the range of possibilities we can see, while keeping us from drifting into unbridled science fiction"* [26]. Each scenario was constructed with input from a base of seven professionals in the financial security sector, and the risks in each were evaluated in accordance with ISO 27005:2008. This was contrasted with the results of a survey with 40 external information security professionals, sourced from academia and industry. The forecasting process comprises six stages, shown in Figure 1, and described as follows:

1. **Plausible Scenario Formulation**: Formulate various situations that explore IoT applications in consumer-centric finance with scenario planning (using the process and scope described in Section 4).
2. **Formalisation**: Identify and categorise threats, vulnerabilities and assets in those scenarios, as per ISO 27005:2008, via the process in Section 5.
3. **Value Assignment**: Assign integers that reflect the likelihood and impact of threats and vulnerabilities, and the value of assets involved.
4. **Internal Risk Evaluation**: Review and evaluate the values in the last step, and computing risk values using the process in Section 5.2.
5. **External Evaluation**: Establish existing judgements relating to IoT security using a survey with external participants, as described in Section 6.1.
6. **Insights and Conclusions**: Produce insights via comparative analysis and formulate recommendations.

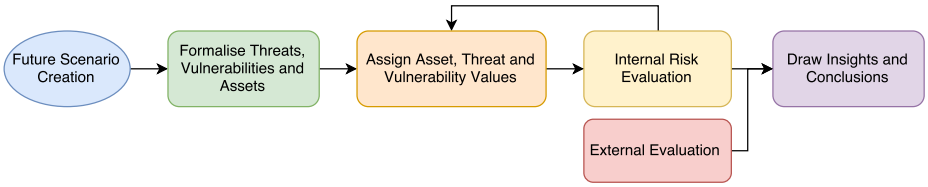

Fig. 1. High-level risk analysis process.

4 Scenario Formulation

The focus of this work is consumer-oriented financial products. We concentrate on end-users and their relationship with financial institutions; we do not directly consider bank personnel or the internal workings of financial institutions. While these too are likely to be impacted by IoT, we believe that this will be shared by most service industries. The timeframe for our investigation is limited to the present to near-future (approximately 5 years) to incorporate emerging IoT technologies that may become mainstream. Where available, we refer to real-life examples of emerging IoT products explored by financial services, e.g., as demonstrations or in white papers.

Similar to [2], three scenarios were created using an iterative approach that, firstly, identified locations where IoT could be applied, e.g., while in-store, at home or in a bank's branch; secondly, listing plausible and relevant IoT technologies in such locations; and, thirdly, identifying financial products that could leverage such technologies in those locations. The locations, actors, IoT technologies and chosen financial products were revised between scenario creators and reviewers. This cycle was repeated until all implausible IoT applications were removed, before formalising the associated assets, threats and vulnerabilities. Note, however, that security threats regarding a smartphone owned by other entities in the scenario, such as a fellow shopper in a supermarket, for example, were not considered. The scenarios are summarised in the following sub-sections. We explicitly list the financial products and the IoT applications in each scenario in Table 1. Given the timeframe of the scenarios, we made the conservative assumption that communication and architectural methods would not change radically. We make regular use of current, standardised methods of short-range communication (e.g., Bluetooth, RFID and NFC), long-range communication (WiFi and 4G) and architectures (e.g., client-server model mediated by an HTTP API).

Scenario A. Follows a technically-adept international businesswoman suffering from a chronic health condition. The scenario explores the use of sensor-equipped pillboxes that monitor drug consumption to assist with adherence[3]. Her adherence is used to price her health insurance premiums by streaming the data through her smartphone, via Bluetooth, to a remote service via 4G or WiFi. The scenario also covers the use of IoT to monitor business information from her employer through RFID in the supply chain, where stock data and market prices are streamed to a smartwatch client. Business shipments are tracked using a blockchain managed by freighters, importers and exporters for implementing smart contracts. Frictionless payments are explored while driving when pre-ordering coffee using an in-car, Internet-connected dashboard to retrieve at a roadside store. The scenario captures tracking lost or stolen insured items by placing GPS/location modules into valuables, such as a watch or necklace, that streams coordinates to a remote recovery service.

Scenario B. Observes a family supermarket trip, exploring the use of product recommendation using a system that learns past behaviour; frictionless payments with RFID-equipped items, avoiding the need to queue at checkouts; and targeted advertising using in-store beacons, which push discounts via Bluetooth LE[4]. The scenario examines emerging budgeting methods that monitor energy consumption from smart home appliances. This is enabled by streaming data to a LAN-connected hub, which is accessible to a mobile client. The owner may control these appliances by activating eco-/power-saving modes to reduce operating cost. In-vehicle commerce is also explored to pay for charging points

[3] AdhereTech is one example of sensor-enabled pillboxes (`https://adheretech.com`)

[4] Beacons track users' in-store location and push notifications to connected mobile devices. Beaconstac is one such example (`http://www.beaconstac.com/retail`).

with electric cars using a credit account stored on the driver's phone, as well as proposing optimal loan terms from past spending behaviour.

Scenario C. Observes a retired man and the effects of evolving demographics on banking with respect to technological resistance and technical illiteracy. The scenario captures managing multiple bank accounts from a single wearable device (service centralisation) and in-branch Bluetooth beacons for displaying offers, assessing customer footfall, and clerk/appointment notification. Vehicle telematics is investigated for accurately pricing motor insurance, where sensor data – car location, speed and driving aggression – is streamed to a remote insurance server over a 4G mobile network. Additionally, continuous authentication and NFC-based access control is explored for accessing bank accounts and in-branch safety deposit boxes with improved usability.

Table 1. Investigated IoT technologies and products and services.

Product/Service	**IoT Applications & Related Work**
Scenario A	
Health insurance	Personalised pricing from physiological sensor data [19]; Drug adherence monitoring [23];
Business analytics	RFID in financial supply chains [17]; Sensor-equipped warehouses [39]; Smart contracts in international trade [12];
Motor insurance	Premium pricing from vehicle telematics [28];
Frictionless payments	Car-based commerce* [4]; Ubiquitous contactless payments†;
Targeted advertising	Localisation with Bluetooth beacons [10];
Insurance forensics	Tracking sensor-equipped valuable items [25];
Scenario B	
Price comparison	RFID-tagged store items [22];
Product recommendations	Learning from in-store item interactions [37];
Frictionless payments	Automated item replenishment from appliances [15]; Automated checkout with RFID-tagged items [22];
Budgeting services	Adapting home energy consumption to budget [5];
Frictionless payments	Car commerce [4];
Targeted advertising	In-store beacon technology [10];
Scenario C	
Bank account management	Centralisation of retail banking services on wearable devices; Continuous, sensor-based authentication [31]; NFC access control for 'smart' bank safety deposit boxes;
In-branch experience	Beacon technology [10];
Motor insurance	Vehicle telematics [28].

* Car commerce is the ability to initiate in-vehicle financial transactions.

† Ubiquitous payments refer to NFC-type contactless payments in public places, e.g., purchasing advertised goods on digital signage using a nearby terminal.

5 Risk Assessment Methodology

The scenarios were formalised into explicit lists of assets, security threats and vulnerabilities, as defined in the following section.

5.1 Definitions

In our assessment, the definitions of assets, vulnerabilities and threats were drawn from ISO/IEC 27005:2008 [1] as follows. Note that typical risk assessments include existing controls; as per [2], we assume their existence and are reflected in the threat, asset and vulnerability values.

Threats are events that endanger an asset via criminal actions, e.g., the interception of network traffic; the environment, e.g., fire and floods; or accidental actions, such as through human error. Each was given a value between 1–5 representing its likelihood and noted whether it impacts confidentiality, integrity and availability. Human threats, e.g., criminal behaviour, were approximated from the likely capability and motivation of the threat agent, while the remaining threats were estimated from their perceived likelihood and damage potential.

Assets comprise physical devices, online/corporate services, software applications and data that supports business processes or relate to personal information. Assets were categorised into the following groups: *physical devices*, e.g., wearable devices and smartphones; *data*, such as transaction information, sensor data and access credentials; *services*, i.e. applications required to conduct and support business activity, such as customer databases; and *consumer applications* used by users to interact with business services. Each asset was assigned its owner and an value of 1–5 (low to high) representing its likely value. This value was approximated by considering its replacement value and the following areas based on Marinos et al. [21]: *convenience*, *economic benefit to users*, *time saved*, *energy saved* and *security benefit*. Assets may also be comprised of smaller sub-assets: a smartphone, for example, that contains multiple applications.

Vulnerabilities comprise circumstances that enable a threat to be realised and were categorised into the following groups: *hardware*, *network*, *organisational/governance* (e.g., compliance with regulations), *personnel* (e.g., poor employee awareness) and *software* flaws. Each vulnerability was paired with its relevant assets and assigned an integer between 1–5 denoting the *exposure* of the asset to the vulnerability and the degree to which it may harm an asset (*severity*). A single value was produced by computing the mean of these.

5.2 Risk Calculation

Asset, threat and vulnerability combinations were assessed manually for their plausibility, before discarding illogical triples, e.g., power outages disrupting the confidentiality of passive RFID tags. The final risk list was aggregated from the remaining combinations of assets, vulnerabilities and threats. Following this, the exposure, severity and value numbers for the vulnerabilities, threats and assets were reviewed and revised once more. A single risk value was calculated using the

risk formula in Equation 1, as used in [1]. The matrix shown in Table 2 depicts the range of possible risk values from 1–13, reflecting the ENISA classification system (1: lowest; 13: highest risk) [1,2]. Finally, the mean risk and standard deviation was computed for each asset, threat and vulnerability category in Section 5.1.

$$\text{Risk} = \text{Asset Value} + \text{Vulnerability Value} + \text{Threat Value} - 2 \tag{1}$$

Table 2. Risk score matrix derived from asset, threat and vulnerability values.

Vuln. value		1					**2**					3					**4**					5				
Threat value		1	2	3	4	5	**1**	**2**	**3**	**4**	**5**	1	2	3	4	5	**1**	**2**	**3**	**4**	**5**	1	2	3	4	5
Asset value	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
	2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
	3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
	4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
	5	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13

6 Evaluation

We conducted a survey with 40 participants from the security profession to contrast the results of our internal assessment with existing IoT security opinions.

6.1 Survey Methodology

An online survey was conducted comprising 48 questions that requested participants to judge and rank various assets, threats and vulnerabilities using in-context examples from the scenarios. Given the detail of the internal assessment – over 1,400 risks in total – the survey questions were formed by taking a random sample of assets, vulnerabilities and threats from the scenarios. At least one item was taken from each class sub-group, while remaining within a 10 minute time limit to maximise participation. For threats and vulnerabilities, participants were asked to predict their importance in the context of the scenario, while clearly stating the specified timeframe of the scenarios. For assets, users were presented with a random subset of scenario assets and asked to rank their perceived value to their respective owners. All responses used a 10-point Likert scale, from lowest to highest value. Survey participants were recruited by email invitation via mailing lists for Ph.D. students, alumni and staff of the Information Security Group at Royal Holloway, University of London. Postings to social media networks for security professionals were also made and no further incentive was offered for participation. Users were asked to input their current occupation and their experience – both academic and industrial – within the security profession in years, and their current position.

7 Results

In total, 1,429 risks were analysed across all three scenarios. Scenario A comprised **515** risks with a mean risk $\mu = 8.50$ and standard deviation $\sigma = 1.44$. Scenario B comprised **604** risks ($\mu = 8.24$; $\sigma = 1.45$), while Scenario C contained **310** risks ($\mu = 8.68$; $\sigma = 1.09$). Table 3 summarises the risks across all three scenarios based on asset, threat and vulnerability classes, while Figure 2 illustrates the distribution of risks across all scenarios. Furthermore, we present the top 10 items with the highest risk for each class – assets, vulnerabilities and threats – in Table 4, along with the proportion of these in each scenario in Figure 3.

Forty security professionals responded to our survey, with a mean of $\mu = 6.33$ years experience ($\sigma = 6.78$) in the field, both industrial and academic security experience combined. The survey results were standardised to the risk range in Table 2 (1–13), before conducting a two-sample t-test with the difference of means to determine statistical significance between the assessments. We present this in Table 4. Many concerns found in our work coincide with those previously known; our findings suggest, however, that particular areas are potentially over- and undervalued, and we analyse these forthwith.

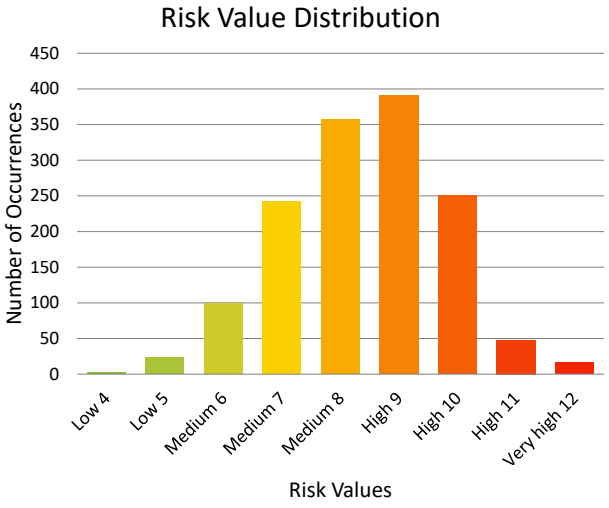

Fig. 2. Distribution of risks across all scenarios.

Untrusted sensing data. Acting on potentially untrustworthy data from remote, unattended devices was a recurring theme in our findings. IoT offers opportunities in automating financial payments and optimising services using sensor data, but the findings suggest this correlates with high risk. Three of the top identified risks concerned trusting sensor data, i.e. 1) improper integrity checks, 2) unreliable sensors, and 3) poor verification/auditing of sensing data to ensure

Table 3. Summary of asset, vulnerability and threat classes across all scenarios.

Class	Mean Risk	Std. Dev.	Occurrences
Assets			
Services	9.40	1.26	233
Applications	8.54	1.15	280
Hardware	8.14	1.35	795
Data	7.97	1.35	121
Vulnerabilities			
Network	9.07	1.43	193
Software	8.55	1.24	649
Organisational	8.24	1.34	432
Hardware	7.19	1.33	155
Threats			
Nefarious activity	8.85	1.06	136
Outages (non-malicious)	7.79	1.12	121
Device reliability	7.88	1.17	129
Data interception and modification	8.78	1.09	546
Organisational	8.43	0.88	215
Physical security	8.42	0.99	101
Unintentional damage and loss	7.52	1.36	181

its veracity. Using data from remote devices at face value is likely to impose significant risk. Data could itself be poor at source: low-cost sensing systems, for example, may simply return inaccurate or unreliable data, but may also be the result of tampering, e.g., a reckless driver tampering with telemetric firmware to transmit 'safer' values to mislead insurers. If systems become largely automated without adequate human oversight and auditing procedures, the consequences may be more severe. Our survey findings illustrate that external experts tended to show a small but statistically significant bias (for $p < 0.05$) towards undervaluing the risk imposed by untrusted sensing data (-0.93; $p = 0.04$). This is further exhibited by assets that receive and transmit such data – asset 2: *investment database*, and asset 4: *freight communication device* – both of which were significantly under-appreciated in the expert survey (-3.13 and -2.37 respectively; $p < 0.01$). Consequently, we recommend particular attention be given to oversight when trusting data from remote, unattended devices at scale.

Authentication. Unsurprisingly, authentication issues – both user and device authentication – consistently yielded the highest risk for both vulnerabilities and threats across our studies (9.22–10.67), comprising aspects such as unauthorised device pairing, permitting weak passwords, and the absence of multi-factor authentication. Consequences of poor authentication vary widely, from obvious examples of unauthorised use of banking and shopping applications, to allowing unauthorised users to pair with sensitive devices, such as for healthcare. Evidently, IoT authentication is complicated by the need for providers to authen-

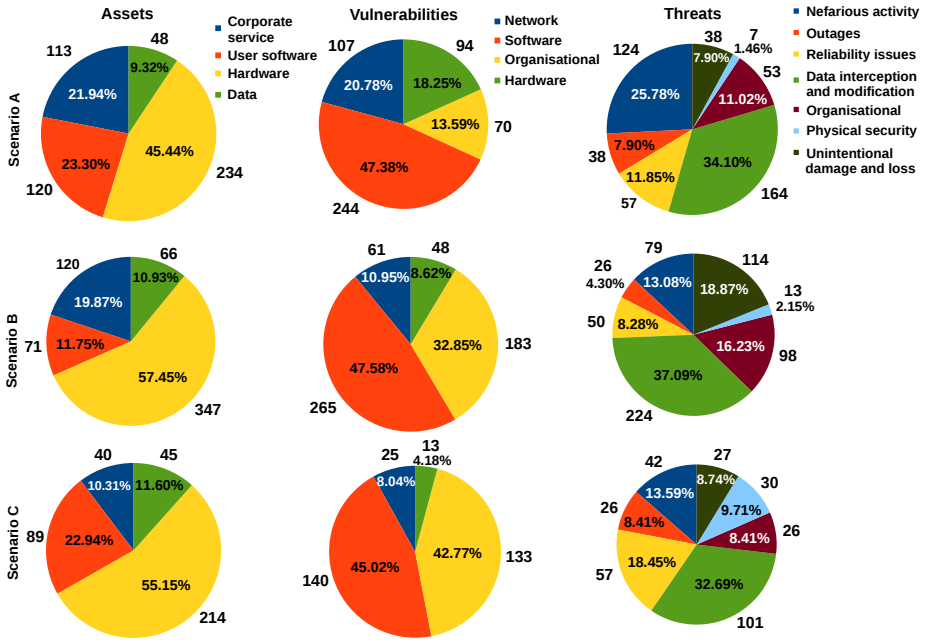

Fig. 3. Distributions of asset, vulnerability and threat classes.

ticate both customers, their devices and any intermediary services, e.g., cloud providers, which may operate with a large degree of autonomy.

Hardware and physical protection. A related observation is the correlation of poor device hardware security with high risk. Remote IoT devices, potentially under users' control, gives rise to the opportunity for adversaries (who could be users themselves) to interrogate devices without the deterrent of human detection. Noticeably, this contributes directly to the first theme. Inadequate physical protection may enable attackers to access the device PCB to tamper with sensing hardware, such as through unauthorised firmware flashing via unsecured interfaces, e.g., UART or JTAG; replacing hardware with purposefully defective components; and adding unauthorised components to bypass existing security controls ('modchip' attacks). Such vectors could be exploited to deliver inaccurate measurements to an insurer or other receiving financial entity. Concurrently, devices themselves may be of significant value (including the data they hold) and hence a target for theft, e.g., smartwatch,. Both hardware tampering and poor physical security ranked in the top 10 threats and vulnerabilities (7.38 and 7.08 respectively). Survey participants marginally undervalued physical theft as a threat (-0.76; p=0.04), but somewhat overvalued hardware tampering (+2.45; $p < 0.01$). We recommend giving physical security high prominence in an IoT system design, particularly when placed remotely.

Table 4. Comparison of top ten mean risks from assets, vulnerabilities and threats of the internal assessment with the user survey, with mean differences and t-test p-values.

Class	Internal	Survey	μ-Difference	t-test$_p$
Assets				
1. Card payment data	11.00	11.79	+0.79	0.35
2. Investment database	10.58	7.71	-3.13	<0.01
3. Online banking service	10.05	11.88	+1.83	<0.01
4. Freight communication device	9.50	7.13	-2.37	<0.01
5. Customer location data	9.25	5.83	-3.42	<0.01
6. Coffee store purchasing service	9.22	9.92	+0.70	0.08
7. Investment mobile app	9.15	8.21	-0.94	0.09
8. Remote insurance service	9.14	8.34	-0.80	0.16
9. Smart safe	9.05	9.75	+0.70	0.32
10. Car operating system	9.00	10.58	+1.58	0.03
Vulnerabilities				
1. Poor user authentication	9.22	10.58	+1.36	<0.01
2. Software network vulnerabilities[†]	9.27	11.29	+2.02	<0.01
3. Poor auditing of remote data	9.11	8.58	-0.53	0.22
4. Poor data integrity protection	9.04	9.54	+0.54	0.16
5. Poor logical access control	8.86	10.50	+1.64	<0.01
6. API vulnerabilities	8.76	10.79	+2.03	<0.01
7. Unreliable sensors	8.60	7.67	-0.93	0.04
8. Poor self-correction mechanisms[^]	8.55	8.50	-0.05	0.91
9. Unfriendly user interface	7.88	9.92	+2.04	<0.01
10. Poor Physical Security	7.08	8.13	+1.05	<0.01
Threats				
1. Authentication issues	10.10	10.67	+0.57	0.13
2. Transaction data modification	9.64	10.75	+1.11	0.01
3. Denial of Service	9.38	10.25	+0.97	0.03
4. Privacy violations[$]	9.19	11.54	+2.35	<0.01
5. Physical theft	9.18	8.42	-0.76	0.04
6. Data and identity theft	9.00	10.92	+1.92	<0.01
7. Use of inaccurate of data	8.89	8.58	-0.31	0.37
8. Service unavailability (non-malicious)	8.78	8.38	-0.40	0.33
9. Malware	8.67	11.63	+2.96	<0.01
10. Hardware tampering	7.38	9.83	+2.45	<0.01

[†] Software network vulnerabilities comprises risks such as exposed and unprotected networking ports and services running on a device.
[$] Privacy violations comprise unauthorised customer profiling and tracking.
[^] Self-correction refers to users' ability to undo/reverse automated transactions.

Data governance. One significant theme expectedly surrounded data protection and adequate measures for disposing obsolete and superfluous data. The access to potentially sensitive data enabled by IoT devices may lead to abuse, whether intentional or unintentional, such as through unauthorised profiling and tracking via beacons and other location techniques. Moreover, with potentially large volumes of data, customer data may be retained longer than necessary or over-collected without adequate oversight – exposing firms to risks surrounding over-sharing, loss and theft. IoT also has the potential to exacerbate existing data protection concerns: valuable data initially collected for one purpose, e.g., self-monitoring home energy consumption, may easily be used for another without consent, e.g., targeted advertising of new, energy-efficient appliances. Participants undervalued the risks posed by customers' location data (-3.13; $p < 0.01$), but appreciated the risks imposed by privacy violations, such as unauthorised profiling (11.54), and identity theft (9.00–10.92).

Interception/modification of transaction data. Expectedly, interception of transaction data from IoT devices yielded high risk (9.64–10.75). While paying for RFID-equipped goods without waiting sounds attractive, or smart appliances automatically replenishing items, these transactions make obvious targets for attackers. Such attacks – the result of inadequate encryption, integrity protection and secure credential storage – are neither new nor specific to IoT, and are known widely by the community. The risks, however, could be exacerbated when considering limited, smaller-scale devices manufactured at a minimal price per unit ($< \$0.05$), which may be incapable of secure tamper-proof credential hosting, or secure encryption at acceptable speeds.

7.1 Limitations

A number of assumptions were made to scope scenario creation: cryptocurrencies, e.g., Bitcoin, were not sufficiently captured. Such currencies typically eliminate or replace financial services altogether; for this study, focus was concentrated primarily on the role of IoT in traditional services. Importantly, we do not claim that our scenarios are exhaustive of all financial services, and our work should be treated with caution in other domains. Moreover, our results should not be over-interpreted as a definitive risk assessment; rather, we aim to provide indications of potential areas of focus. Like with any risk assessment work, comes uncertainty: biases may be present from the professionals in this work, but we attempted to mitigate this through a large user-base with input restricted to informed professionals. Note that risk assessments take intense effort to conduct correctly, and a survey is not sufficient to digest the described scenarios entirely; we reiterate that the external survey was used to capture and contrast opinions on IoT in finance and was not a fundamental component of the assessment itself.

8 Conclusion

In this work, we introduced the need to robustly assess potential security risks associated with use of IoT in financial products and services. This was succeeded

by an examination of related work in mobile and cloud computing, healthcare, and RFID in air travel, before describing a high-level framework using scenario planning and ISO 27005:2008 from past work. A range of related scenarios were developed with consultation from domain experts, which incorporated a variety of emerging IoT technologies and financial applications. After formalising the threats, vulnerabilities and assets in each scenario, a total of 1,429 risks were identified. We contrasted these results with an external survey with 40 security professionals, both in academia and industry, with the aim of capturing existing opinions on IoT security. From this, we identified and analysed several areas of concern that are likely to take precedence in the field. The results are presented in order to assist future research, policy formulation and decision making.

8.1 Future Research

Subsequent to this work, we hope to pursue the following avenues of research:

- Investigating the potential security risks associated with cryptocurrency use in IoT deployments.
- Capturing the risks of machine-to-machine payments and unconventional technologies for frictionless payments, such as implantable devices.
- Incorporating unique financial interactions with multiple actors, such as group payments and peer-to-peer lending.

Acknowledgements The authors would like to thank those at Vasco Data Security, who initiated and supported this work; the participants of the user survey for their time and consideration; and the anonymous reviewers who provided their insightful and helpful comments. Carlton Shepherd is supported by the EPSRC and the UK government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/K035584/1).

References

1. *BS ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management.* British Standards (BSI), June 2008.
2. Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology. Technical report, European Network and Information Security Agency (ENISA), 2010.
3. ENISA EFR Framework - Introductory Manual. Technical report, European Network and Information Security Agency (ENISA), Mar. 2013.
4. Accenture. Connected commerce hits the road, 2016. `https://www.accenture.com/be-en/success-visa-connected-commerce-car`.
5. D. Alahakoon and X. Yu. Smart electricity meter data intelligence for future energy systems: A survey. *IEEE Transactions on Industrial Informatics*, 12(1):425–436, 2016.
6. W. Bodwell and T. J. Chermack. Organizational ambidexterity: Integrating deliberate and emergent strategy with scenario planning. *Technological Forecasting and Social Change*, 77(2):193–202, 2010.

7. G. Cairns, G. Wright, R. Bradfield, K. van der Heijden, and G. Burt. Exploring e-government futures through the application of scenario planning. *Technological Forecasting and Social Change*, 71(3):217–238, 2004.
8. Capgemini. Wearable Devices and their Applicability in the Life Insurance Industry, April 2014. `https://www.capgemini.com/resource-file-access/resource/pdf/wearable_devices_and_their_applicability_in_the_life_insurance_industry.pdf`.
9. M.-S. Chang, Y.-L. Tseng, and J.-W. Chen. A scenario planning approach for the flood emergency logistics preparation problem under uncertainty. *Transportation Research: Logistics and Transportation*, 43(6):737–754, 2007.
10. S. S. Chawathe. Beacon placement for indoor localization using Bluetooth. In *11th International IEEE Conference on Intelligent Transportation Systems*, pages 980–985. IEEE, 2008.
11. DHL. Internet of Things in Logistics, 2016. `https://www.scribd.com/document/285437514/DHL-TrendReport-Internet-of-Things`.
12. R. Franklin, A. Metzger, M. Stollberg, Y. Engel, K. Fjørtoft, R. Fleischhauer, C. Marquezan, and L. S. Ramstad. Future internet technology for the future of transport and logistics. In *European Conference on a Service-Based Internet*, pages 290–301. Springer, 2011.
13. Gartner, Inc. 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015, November 2015. `http://www.gartner.com/newsroom/id/3165317`.
14. M. Gren. Finance Stock Watch on Google Play, 2016. `https://play.google.com/store/apps/details?id=com.mathck.android.wearable.stoc`.
15. H. Gu and D. Wang. A content-aware fridge based on RFID in smart home for home-healthcare. In *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, volume 2, pages 987–990. IEEE, 2009.
16. IBM. IBM Watson IoT for Insurance, 2016. `http://www.ibm.com/internet-of-things/iot-solutions/iot-insurance/`.
17. T. Inaba. Impact Analysis of RFID on Financial Supply Chain Management. In *IEEE International Conference on Service Operations and Logistics, and Informatics*, pages 1–6, Aug 2007.
18. C. W. Karvetski, J. H. Lambert, and I. Linkov. Scenario and multiple criteria decision analysis for environmental security of military and industrial installations. *Environmental assessment and management*, 7(2):228–236, 2011.
19. S. Kumara, L. Cui, and J. Zhang. Sensors, networks and internet of things: research challenges in health care. In *Proceedings of the 8th International Workshop on Information Integration on the Web*, page 2. ACM, 2011.
20. L. Lewis and J. Wyatt. mHealth and Medical Apps: A Framework to Assess Risk and Promote Safer Use. *J Med Internet Res*, 16(9):e210, Sep 2014.
21. Louis Marinos. ENISA Threat Taxonomy - A tool for structuring threat information. Technical report, European Union Agency for Network and Information Security (ENISA), Jan. 2016.
22. J. Melià-Seguí, R. Pous, A. Carreras, M. Morenza-Cinos, R. Parada, Z. Liaghat, and R. De Porrata-Doria. Enhancing the shopping experience through RFID in an actual retail store. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing*, pages 1029–1036. ACM, 2013.
23. J. Morak, M. Schwarz, D. Hayn, and G. Schreier. Feasibility of mhealth and near field communication technology based medication adherence monitoring. In *2012 IEEE International Conference on Engineering in Medicine and Biology*, pages 272–275. IEEE, 2012.

24. E. S. Nadimi, R. N. Jørgensen, V. Blanes-Vidal, and S. Christensen. Monitoring and classifying animal behavior using ZigBee-based mobile ad hoc wireless sensor networks and artificial neural networks. *Computers and Electronics in Agriculture*, 82:44–54, 2012.
25. NXP Semiconductors, FreeScale and ARM. What the Internet of Things (IoT) needs to become a reality, 2013. `http://www.nxp.com/assets/documents/data/en/white-papers/INTOTHNGSWP.pdf`.
26. Paul J. H. Schoemaker. Scenario planning: a tool for strategic thinking. *Sloan Management Review*, 36(2):25–40, Jan. 1995.
27. PwC. Connected insurance, 2016. `https://www.pwc.com/it/it/publications/assets/docs/connected-insurance.pdf`.
28. RAC Limited. Black box car insurance, 2017. `http://www.rac.co.uk/insurance/car-insurance/black-box-insurance`.
29. Salesforce. Introducing Salesforce IOT Cloud, 2016. `http://www.salesforce.com/uk/iot-cloud/`.
30. P. Saripalli and B. Walters. Quirc: A quantitative impact and risk assessment framework for cloud security. In *3rd International Conference on Cloud Computing*, pages 280–288. IEEE, 2010.
31. C. Shepherd, R. N. Akram, and K. Markantonakis. Towards Trusted Execution of Multi-modal Continuous Authentication Schemes. In *Proceedings of the 32nd ACM Symposium on Applied Computing*, pages 1444–1451. ACM, 2017.
32. F. Shrouf, J. Ordieres, and G. Miragliotta. Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In *IEEE International Conference on Industrial Engineering and Engineering Management*, pages 697–701. IEEE, 2014.
33. Tata Constultancy. Banking and Financial Services: Pleasing Customers, Fighting Fraud, 2016. `http://sites.tcs.com/internet-of-things/industries/banking-and-financial-services/`.
34. M. Theoharidou, A. Mylonas, and D. Gritzalis. *A Risk Assessment Method for Smartphones*, pages 443–456. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
35. U. Varshney. Pervasive healthcare and wireless health monitoring. *Mobile Networks and Applications*, 12(2-3):113–127, 2007.
36. A. Volkery and T. Ribeiro. Scenario planning in public policy: Understanding use, impacts and the role of institutional context factors. *Technological forecasting and social change*, 76(9):1198–1207, 2009.
37. F. Von Reischach, D. Guinard, F. Michahelles, and E. Fleisch. A mobile product recommendation system interacting with tagged products. In *Pervasive Computing and Communications*, pages 1–6. IEEE, 2009.
38. Z. Yan, P. Zhang, and A. V. Vasilakos. A survey on trust management for IoT. *Journal of Network and Computer Applications*, 42:120–134, 2014.
39. Z. Zhang, Z. Pang, J. Chen, Q. Chen, H. Tenhunen, L.-R. Zheng, and X. Yan. Two-layered wireless sensor networks for warehouses and supermarkets. In *3rd International Conference on Mobile Ubiquitous Computing, Systems, Services, and Technologies*, pages 220–224, 2009.