International Journal of Technology and Human Interaction
Volume 18 • Issue 7

Building and Bridging Security and Privacy-Related Technical Knowledge Amongst HR Professionals:
A Review in the Context of Industry 4.0

Anuragini Shirish, Université Paris-Saclay, Univ Evry, IMT-BS, LITEM, Evry-Courcouronnes, France*
https://orcid.org/0000-0001-8199-2889

Priya Jyoti, Institut Mines Telecom Business School, France

ABSTRACT

An ever-increasing range of smart, connected internet of things (IoT) devices poses entirely novel security and privacy challenges. Business models that wish to rely on smart product adoption will need to ensure the capability to deliver systems that offer adequate data integrity of sensors with the guarantee of privacy for users. Incorporating smart devices into the mainstream internet poses many security problems, as most internet technologies and protocols have not been developed to support IoT. Strategic support units such as human resources need sufficient technical knowledge about the state of the art to navigate and leverage Industry 4.0 into their practices. Human resources professionals are increasingly asked to take strategic and not operational roles. Using a systematic review method, the authors expose the security and privacy challenges posed by IoTs and conclude with a framework that maps potential solutions to the identified problems. The framework adds to the strategic HR literature and practically helps improve the technical acumen of human resource professionals.

KEYWORDS

Blockchain, Digital Work Practices, Human Resource Systems, IoT, Mobile Fog, RFID, Systematic Literature Review, Technical Competence

INTRODUCTION

Businesses have adapted to several important technology driven waves of change in societies, starting from lean revolution around 1970s, the outsourcing possibilities that offered new business models to develop in the 1990s and the automation that penetrated in the 2000s. The latest of these trends is the integration of cyber-physical systems such as use of internet of things (IoT) to increase revenue and drive cost reductions (Rymaszewska et al., 2017). It also facilitates both consumer driven markets and industry 4.0 powered by innovative operational technologies (OT) of which IoTs are a part. It allows for manufacturing processes and operations to assimilate and develop a flexible, smart, cost effective, eco-friendly and socially responsible production ecosystem (Metallo et al., 2018; Oesterreich

DOI: 10.4018/IJTHI.306225 *Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

& Teuteberg, 2016; Strazdins & Wang, 2015). However, there is a lack of built-in security in cyber-physical systems, thus security and privacy issues loom high in the IoT domain. It can result in unauthorized access to services and data, exposure of key enterprise elements, compromise private data, be prone to denial of services, backdoors and malwares, as well as face loss or damage to critical human resource infrastructure. Thus, before enterprises leverage IoT and integrate it into their business models or incorporate them as a strategic resource in human resource management, they must be prepared to handle two critical aspects. First, protecting communication through IoTs and second, managing security configurations and credentials (Pfaff, 2020). Knowledge about these aspects contributes to bridging the technical deficiencies often seen amongst human resource professionals.

Recent research also project that human resource domains will be highly influenced by IoTs, but they can also influence in bring about positive change within organizations due to IoTs. Thus, human resources are impacted by IoT related issues and can play various roles such as a potential change agents, a change drivers and most importantly as a strategic partners. As a change agent, human resources are primarily responsible for how communication, privacy and security issues are managed between employees and mediated systems. They also provide the best practices for better organisational communication, privacy and security (Strohmeier, 2020). As a change driver, human resource functions may itself be impacted by IoTs. Prior studies project that a combination of e-HRM with IoTs have wide applications for implementing policies, strategies, and practices within the organization in five crucial areas of e-Selection, e-Recruitment, e-Performance, e-Compensation, and e-Learning (Nasar, et al., 2020). However, as a strategic partner, they need to build their dynamic capability and knowledge base in order to adapt to the ever changing technological environment caused by industry 4.0 trends. This requires them to constantly update their technical knowledge to overcome the constant state of deficit they find themselves in the face of IoT related challenges to effectively contribute at the strategic levels in the organizations. Thus, in order to successfully make this expected transition from a traditional operational function to a strategic function within industry 4.0 oriented organizations (Hecklau et al., 2016) human resource professional need to bridge this technical gap with regard the management of privacy and security challenges in IoT.

They predict that there will be over 75.44 billion IoT devices worldwide by 2025 and their role in cyber-physical systems gives rise to several important security concerns[1]. Internet of Things or (IoT) security and privacy is a trend-setting research area that attracts academic, industrial, and government researchers. Attacks on IoT systems are fast and simple to carry out at the same time there is a rapid expansion of IoT devices in the market, from fitness to relators, making this issue relevant and time sensitive.

In order to address this practical need of the industry and to protect communication and manage security when implementing IoTs in business process, human resource services and digital products, we conduct a structured literature review on this phenomenon enabling us to identify the technological solutions for better management of these issues. Further, the findings of the study can help increase the technical acumen of human resource managers grappling with how best to leverage IoTs for human resource management as well as within the organization as a whole. Prior technology knowledge of human resource experts impact how they handle privacy issues and devise appropriate practises such as provision of prior notices when handling intrusions by IoT technologies both in traditional and in non-traditional work context (Kaupins and Coco, 2017). Thus the specific research questions addressed by this study are, from the perspective of an enterprise:

RQ1: What are the security and privacy challenges due to use of IoTs that human resource professionals need to know?
RQ2: How can we overcome these challenges?

The paper is divided into several sections. The first section tackles the background literature. This is followed by the methods section. In this section, we describe the systematic review methodology

in detail. The third section will present the data analysis and the results of the literature review. In the fourth section, a discussion of the main results, theoretical and practical implications are offered. Last section deals with concluding remarks.

BACKGROUND LITERATURE

Internet of Things: Security and Privacy Issues

IoT is a series of "things" embedded with electronics, software, sensors, actuators and linked to each other through the Internet to collect and exchange data (Ranger,2020). The IoT devices can be remotely controlled to perform the desired functions (Chanson et al., 2019). The sharing of information between the devices takes place via the network, which uses standard communication protocols. IoT uses the cloud to process data generated by networks of edge sensors and offers services to users at the upper-level (Buyya, 2016). The users can do the collection, processing, analyzing and storing of data on demand (Yi et al., 2015). The security and privacy aspect of IoTs can impact human resource managers. We expect the three areas of human resource configuration as discussed in the literature to be affected as per a recent exploratory survey among human resource experts (Strohmeier, 2007, 2020). IoTs can influence and interact to impact human resource actors, human resource technology, and human resource activities within an organization (Strohmeier, 2020). Thus it becomes important to understand how to manage these emergent challenges from strategic human resource management perspectives.

In recent years, there has been a tremendous effort to address security problems in the IoT paradigm. Some of these approaches address security issues at a particular layer, while other approaches seek to provide end-to-end IoT protection (Juma et al., 2020). Some recent research describes security concerns in terms of use, infrastructure, communication, and data (Liehuang Zhu, 2017; Sicari et al., 2015). This proposed IoT safety taxonomy differs from conventional layered architecture. Similarly, another study addresses and analyses security issues for the defined IoT protocols (IEEE, 2020). Few propose a comparative evaluation of systems for detecting intrusion using Fog computing (Yi et al., 2015). While others address contributions to IoT that include confidentiality, protection, access control and privacy along with middleware protection (Sicari et al., 2015). Overall, main issues that these authors addressed were trust management, authentication, privacy issues, data security, network security, and intrusion detection systems.

Security and privacy remain big challenges for IoTs, which pose a completely new dimension of user privacy issues. It can also implicate employees of organizations as well as give rise to ethical issues (Kaupins and Coco, 2017). This is because IoTs not only collect personal information, such as usernames and phone numbers but can also track user activity like their habits and routines. Following the endless string of leaks concerning major data breaches, customers are apprehensive about sharing personal data in public or private clouds, for good reasons[2]. Human resource managers are also sceptical to use IoTs even for ethical monitoring scenarios (Kaupins and Coco, 2017). Therefore, the current study reviews the latest security and privacy challenges in IoT and the different solutions to overcome the challenge to throw light into this important phenomenon.

METHODOLOGY

There are several types of literature reviews that are undertaken in academic research. Broadly they are categorized into narrative, domain oriented, meta-analysis and systematic literature reviews (Okoli and Schabram 2010; Webster and Watson 2002). A literature review is undertaken with a goal to synthesize, identify important biases and research gaps from the past knowledge about a topic or domain to propose future research directions (Rowe 2014). Systematic literature review is one form of literature review that is undertaken to obtain comprehensive knowledge about a chosen domain

and is often referred to as a form of secondary study with a view to identify, analyze and interpret all available research related to a specific research question (Kitchenham 2007). For achieving these objectives, it is imperative to have a methodology that is unbiased, rigorous, and auditable (Kitchenham et al., 2010).

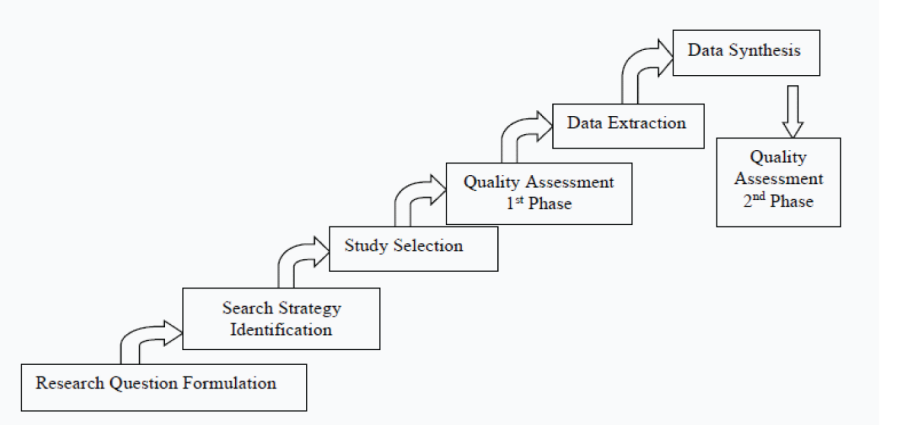
For the current study, conducting a systematic literature was appropriate as it will help to determine in a comprehensive manner, the state of research about the phenomenon being researched; security and privacy issues in IoT, despite its cross disciplinary nature. Moreover, an initial scoping review that was conducted prior to this review clarified the domains involved and identified the seminal works and the background works that are pertinent to the understanding of the 'Internet of things' and 'Security and Privacy' concepts. This further guided the structured review in the form of a systematic literature review (SLR) as it that can help understand the link between the intersecting domains of management and computer science in a thorough manner to identify the potential research areas for further exploration.

This SLR is based on the original guidelines proposed by Kitchenham & Charters (2007) and Okoli and Schabram (2010). Undertaking systematic review has been linked with the ability to extensively search modern digital libraries. This allows for the replicability of the research, which is one of the cardinal principles of undertaking any scientific enquiry. The current study is limited to providing a systematic literature review of the papers that exclusively touch upon the research objectives of this study in order to identify the potential coverage that exists in the current literature specific to the understanding of those questions. Undertaking an exhaustive literature review is often considered as a resource intensive task requiring manpower, finances, and time so we choose to delimit the scope of the literature review (Tandalam Aswinikumar, 2016), the steps used for the systematic literature review undertaken are exhibited in Figure 1.

Research Question Formulation and Search Strategy Identification

We used the research questions of this study as the basic starting point. In the next step we identified the keywords or subject terms that will be used to screen relevant academic material from the online databases. Per prior studies, using basic terminology recognized by the community to identify these terms would suffice (Tandalam Aswinikumar, 2016). Hence, we simply used the string "internet of things" and "security" and "privacy". We decided that higher-order terms which may nest sub-terms are crucial for the study and would provide more comprehensiveness to the review and thus avoid

Figure 1. Steps taken during the systematic literature review



the search to become too narrow in its scope. We used Boolean AND to link the major search terms relevant to the research questions to obtain maximum depth to the research process.

The search terms are cross-disciplinary, so with a view to conduct a comprehensive search, restrictions were introduced for the type of publications, but we restricted the search to 2010- 2020 (May). We conducted the search in digital libraries using EBSCO Host interface, which is a multi-motor search engine comprising databases covering fields of management, social science, humanities, and pure sciences. Using EBSCO host interface also helped in eliminating duplicate material.

To ensure that all studies are analysed consistently, we specified rules about study characteristics, i.e. those that included problems and solutions for security and privacy challenges in IoT. The search strings were entered in the interface under the "advance search" option based on search strategy that was chosen and relevant articles that were available in digital format were extracted. Therefore, the results were retrieved from all fields, including Abstracts, Subject Terms (keywords), Journal Title, Journal Source and Full Text (if available in HTML format and not PDF format). The interface allowed storing the data in online temporary folders which were later transported to reference manager. The search was repeated if a new data extraction strategy was used for the secondary search attempts and a similar process was undertaken to store the results. Once the results were stored, we manually selected the links to every article and downloaded the same in private working folders to further undertake a review of the papers. The described process was adopted for all the search combinations that were chosen for the study.

Study Selection, Quality Assessment Phases, Data Extractions

Keeping in view the newness of the researched phenomenon examined in this study, for accuracy and quality of search process, whenever the primary search results exceeded 150 in number, a secondary search strategy was used to further refine the search to screen and collect pertinent results. More details about the secondary search process are provided under 'quality assessment' section. Secondary search or screening was required to ascertain for the quality of the searched papers. This was especially necessary because of the large number of results that were retrieved during the primary search process. The purpose of quality assessment is to establish rigor and credibility in the literature search process (Chen and Macredie, 2010). There are several ways in which one can enhance the quality of the study.

In systematic literature reviews, study selection criteria are used to determine which articles/studies to include or exclude from the review and analysis. The lists gathered from the primary searches were evaluated using the inclusion and exclusion criteria elaborated below. Please note that the review was only limited to published journal articles and few conferences and did not consider grey literature, company journals, unpublished articles or embargoed material, books, etc. We also restricted the search to works written in English and did not cover other languages. These factors could limit findings from this study. Our inclusion criteria were first, the article is from an academic journal (first phase of inclusion). Second, the entire article is written in English (not merely the abstract). Third, the article is published in a peer-reviewed journal. Any article that was referring to search terms with no explicit identification/measurement/conceptualization, then the paper was excluded. Articles that were editorial comments, opinions and reviews, invited reactions and those informing corrections or providing an erratum were excluded. We also excluded articles where the full text is not available in a digital form.

Following this strategy, we had a total of 1,494 academic papers–the quality criteria set allowed us to narrow down the pool to 18 peer-reviewed articles that addressed security and privacy issues within the paper in depth. In order to determine which of them is to be selected, two phases of exclusion stages were carried out, one general exclusion criteria listed above and the second one based on titles and abstract reviewing. We excluded all papers that did not cover either security or privacy aspects about IoT implementation or usage. Amongst these papers, 13 journal paper discussed IoT security and privacy issues and 5 journal papers provided solutions to overcome the problems.

Expanding the Search Strategy to Conferences

Since the topic is an emerging topic, so we widened the search to conference proceedings as well in order to pick interesting and useful article that can add value to this research enquiry. Therefore, we repeated the process which resulted in finding additional 59 conference articles in the first screening which covered mostly very specific conference outlets such as articles from ACM/EDAC/IEEE Design Automation Conference (DAC); International Conference on Privacy and Security in Mobile Systems (PRISMS); International Conference on the Network of the Future (NOF); IEEE World Forum on Internet of Things (WF-IoT); IEEE 16th International Conference on Communication Technology (ICCT); International Conference on I-SMAC papers. Following the quality assessment phases, we further narrowed down the results to 37 academic contributions and after in-depth abstract and paper analysis, we again narrowed the list to 12 papers in total that covered the three aspects that were important for the selection namely: security, privacy along with solutions to these problems pertaining to the IoTs from the perspective of an enterprise. In the below section we detail are findings from these papers.

RESULTS

Data Synthesis and Analysis

Response to RQ1: Security and Privacy Challenges Identified

We provide the findings from the literature review based on the two research questions we set out to study. Referring to the research question 1, RQ1: What are the security challenges in the IoTs? Out of the 27 selected papers, we can find 8 papers detailing the challenges related to security and privacy that is summarized in this section. Table 1 highlights the papers/journals considered for this section.

We note that information security, network security and privacy should be equipped with these basic principles, such as confidentiality, integrity, availability, authentication and authorization (Kraijak & Tuwanut, 2015). The following obstacles to defining and analysing IoT privacy and security was identified by Alqassem & Svetinovic, (2014): First, obstacle is to determine: how to determine which information should be secured, when to secure and to whom access should be given / restricted. Second, obstacle is that IoT comprises multiple technologies and their combination leads to uncertain threats and problems. Third, the rising uncertainty of the environment plays a significant role in solving weaknesses in the safety and protection of the IoT.

The key protection criteria and their subcomponents were outlined in literature too (Vasilomanolakis et al., 2015). As per this source, key protection criteria can be divided them into

Table 1. Academic papers tackling security and privacy challenges in IoT

Papers journals considered for RQ1
A decentralized approach for security and privacy challenges in the Internet of Things (Skarmeta et al., 2014)
A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends(Kraijak & Tuwanut, 2015).
A taxonomy of security and privacy requirements for the Internet of Things (IoT)(Alqassem & Svetinovic, 2014)
On the Security and Privacy of Internet of Things Architectures and Systems(Vasilomanolakis et al., 2015)
Open security and privacy challenges for the Internet of Things(Strazdins & Wang, 2015)
Security and privacy in the Internet of Things: Current status and open issues(Abomhara & Køien, 2014)
A security survey of middleware for the Internet of Things(Fremantle & Scott, 2015)
Security, privacy and trust in Internet of Things: The road ahead(Sicari et al., 2015)

five groups: Network Security, Identity Protection, Privacy, Trust and Resilience. Figure 2 illustrates the relation between the different IoT properties and the security requirements.

A few other researchers Strazdins & Wang, (2015), Abomhara & Køien, (2014) focused their study on authentication and authorization; key distribution and management; safe data transmission; data storage and safe processing; global rules pertaining to the IoT environment. Strazdins & Wang, (2015), Abomhara & Køien, (2014) have described the issues concerning *authentication and authorization.* Since, most of the data gathered through IoT was for restricted user groups or organizations, mechanisms for authentication (including node or user identity) and authorisation (giving appropriate access permissions) are also needed. Non-repudiation and fairness are key problems in the modern IoT environment, in particular for payment. Especially in distributed topologies, it is difficult to handle identities and trust. An optimal node would identify all the nodes in the network that are licensed. A centralized authority (such as a cellular network provider) can be useful as a trustworthy authority which approves others (Abomhara & Køien, 2014; Strazdins & Wang, 2015).

The second area they identified is to do with *key distribution and management*. They opined that data encryption is necessary to ensure both authentication and permitted access. However, setting up and sharing encryption keys between network nodes is one big challenge (Strazdins & Wang, 2015). *Safe data transmission* is the third issue identified. Multiple security attacks can interfere with secure information sharing, thus allowing non-authorized parties to have data access. Far worse could be when fabricated messages may be inserted into the network, or it can interrupt actual data transfer. Eavesdropping attacks in wireless ad hoc networks have recently become a widespread form of security threat, as many adverse attacks do need inspection. It requires safe protocols which provide redundancy and adaptive network reconfiguration to maintain the quality of the transmission channel (Abomhara & Køien, 2014; Strazdins & Wang, 2015).

Next, *data storage and safe processing* is identified as a challenge in the IoT environment. Raw data needs processing and storage. In addition, intermediate IoT system layers and proxies may want to aggregate data before they transmit it to reduce traffic and overhead computation. But the proxies cannot decode the data that is intended for end users and applications. We should use homomorphic encryption protocols in these cases if they meet compatibility and consistency requirements. Homomorphic protocols require the execution without decryption of a certain set of authenticated data operations. Moreover, dedicated hardware tools can be used to ease intense cryptographic calculations and conserve resources (Abomhara & Køien, 2014; Strazdins & Wang, 2015). Lastly, *lack of global rules* is raised as a concern. Due to the international existence of IoT objects, IoT rules must be universal-as they move across borders, especially products. Maintaining separate laws for each nation would prohibit businesses from doing so (Strazdins & Wang, 2015).

Another important paper, Fremantle & Scott and Sicari et al., (2015) defined privacy and security to be occurring at different levels such as the *information, access and functional levels*. At the *information level*, the following criteria should be secure. Firstly, *integrity*: the data received during transmission should not be altered. Second, is *anonymity*: the identity of the source of the data will remain confidential to third parties. Thirdly, it is *confidentiality*: the details should not be accessed by third-parties. They should establish a trusting partnership between IoT devices for the exchange of protected information. Replicated interactions must always be recognisable. Forth, it

Figure 2. IoT properties and security requirements

	Network Security	Identity Management	Privacy	Trust	Resilience
Uncontrolled Environment	•	•	•	• • •	•
Heterogeneity	•	••	•	••	•
Scalability	•	•	••	•	• • •
Constrained Resources	••	•	••	•	•

is *privac*y: during the exchange of data we should keep private information private. Intruders must have difficulty in interfering identifiable information.

At the *access leve*l, we need certain security mechanisms for controlling network access. In particular, the paper proposes the following functionalities in an IoT device. First, *access control*: it ensures authorized users have access to the devices and the network for administrative tasks. Second, *authentication*: it checks whether it allows a computer to enter a network, and vice versa. This is typically the first function a node does when entering a new network. Further, the systems must have excellent protection to prevent safety hazards. Finally, *authorization functionality* is needed. It guarantees that only approved devices and users access network infrastructure or resources.

At the *functional level*, they prescribe guidelines for the conditions for protections. First, it must ensure *resilience*: This applies to network capacity to ensure its networks are secure, even in the event of attacks and failures. Second, *self-organization* capability. This denotes the capacity of an IoT device to change itself so that it can stay operational, even if certain parts fail because of periodic malfunctions or malicious attacks. This brief review of the literature provides us with the main privacy and security challenges that are highlighted in the IoT literature. We move on to review the possible solutions to IoT security and privacy problems.

Response to RQ2: Tackling Security and Privacy Issues in IoT

Referring to the research question 2, RQ2: How to overcome these challenges? The review was primarily based on those papers that could address this issue in depth out of the total 27 papers. We note that 13 papers gave new technology/ techniques to overcome the above mentioned IoTs issues. Table 2 will highlight these papers considered for this section.

Because of space constrained, we do not elaborate on each and every solution proposed and their applicability, but we summarize the proposed solution and how that can used in IoT context. See below Figure 3 for more details.

We also provide in Table 3 a synthesis of our research findings and the applicability of these technological measures to IoT security and privacy challenges.

Table 2. Academic papers tackling security and privacy issues in IoT

Papers considered for RQ 2
Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities(Wang et al., 2019)
RFID as an Enabler of the Internet of Things: Issues of Security and Privacy(Khoo, 2011)
Where Is Current Research on Blockchain Technology?—A Systematic Review(Yli-Huumo et al., 2016)
An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends(Zheng et al., 2017)
KYC Optimization Using Distributed Ledger Technology(Parra Moyano & Ross, 2017)
Emerging Technologies in Computing(Miraz et al., 2018)
Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data(Chanson et al., 2019)
Blockchain for Cities—A Systematic Literature Review(Shen & Pena-Mora, 2018)
A Blockchain Research Framework(Risius & Spohrer, 2017)
Security in IoT-Enabled Spaces(Al-Turjman, n.d.)
Fog Computing: Platform and Applications(Yi, Hao, et al., 2015)
Fog computing and its role in the internet of things(Bonomi et al., 2012)
RFID technology and its applications in Internet of Things (IoT)(Jia et al., 2012)

Figure 3. Authors' developed-three technological solution and IoT needs identified from the literature

Table 3. Authors' developed -In depth classification of three solutions based on the security and privacy challenges of IoT

IoT security and privacy challenges	RFID	Blockchain	Fog computing
Authentication and authorization	Yes	Yes	No
Key distribution and management	No	Yes	Yes
Safe data transmission	No	Yes	Yes
Data storage and safe processing	Yes	Yes	Yes
Global rules	Yes	Yes	No
Safety at access level	Yes	Yes	No
Safety at information level	No	Yes	Yes
Safety at the functional level	Yes	Yes	Yes

DISCUSSIONS AND IMPLICATIONS

Discussions

Through the literature review, we were able to identify not only the security and the privacy challenges posed by IoT to enterprises and business units such as HR, but also identify three technical solutions to handle the issues. Since, research projects human resource is primarily responsible for how communication, privacy and security issues. They are the mediators between employees and mediated systems, they also provide the best practices for the better organisational communication, privacy and security (Strohmeier, 2020). Moreover, human resource functions may itself be impacted by IoTs. Prior studies project that a combination of e-HRM with IoTs have wide applications for implementing policies, strategies, and practices within the organization in five crucial areas of e-Selection, e-Recruitment, e-Performance, e-Compensation, and e-Learning (Nasar, et al., 2020). In this section we expand on the various solutions proposed by literature to address the security and privacy challenges in implementing IoTs in the three specific areas of RFID, block chain and mobile fog computing. These recommendations and reflections are not only useful for any companies planning to strategically deploy the use of IoTs in its business model but it can offer the much needed technical knowledge that is currently lacking amongst domain specific actors such as human resource managers as they will soon be required to contribute to the design and deployment of such tools in the company.

We appraise human resource management tasks to have great potential for organizational innovation and performance when they leverage IoT knowledge (Strohmeier, 2020; Kaupins and Coco, 2017. Naser et al., 2020). This study adds to other studies such as Loukil et al.,2017 who have examined the IoT-specific solutions considering the security property and requirement fulfillment and studying privacy principle coverage in general. It also adds to other studies such as Ziegeldorf et al. 2014 that look at IoT related issues from a privacy preserving lens by focusing on analyzing the challenges and threats of IoT in the context of entities and information flows. We update the findings concerning security and privacy with regards to IoT for an enterprise or business unit such as HR.

Moreover, we contribute to recent streams of human resource literature that have started to look at the crucial role of human resource in the success of IoT adoption, implementation within an organization (Dhanpat et al., 2020) and the need to build dynamic capability within the organization to thrive in an ever changing IoT innovation environment (Shamim et al., 2016). Understanding technical nuances of the innovative climate in IoT is proposed as a starting point in honing such as dynamic capability. Human resource wear the hat of a change agent as well as strategic change partner. However, one key challenge that stops human resource units to level up to a strategic position is the lack of comprehensive technical skills in IoT related matters that are needed to switch from operational to more strategic tasks (Hecklau et al., 2016).

Thus, we also add to the current literature in human resource that attempts to scope the role of human resource unit in the context of industry 4.0. A review paper expands on the role of human resource in IoT but it limited to the traditional roles of recruiting the right employee for IoT operations. Six human resource practices for developing an Operator 4.0 have been identified: staffing, job design, training, performance appraisal system, knowledge management, and compensation (Margherita and Bua, 2021). This review helps develop the strategic role of human resource but equipping them with technical knowledge and process understanding that will help them to qualitatively contribute to strategic decision making when IoTs are developed and implemented in the organizations. This will enable them to involve in innovation and knowledge management processes confidently. The review identifies latest state-of-the-art solutions to tackle the looming privacy and security problems and it elaborates on the practical feasibility of such solutions in a critical manner to inform human resource practitioners in a concrete way. It adds to other similar studies that tackle the theoretical and practical aspects that have been discussed in industry 4.0 related recent research as well (Bag and Pretorius, 2020; Bag et al., 2021).

Implications and Future Perspectives

We classify human resource roles as change agent, change driver, and strategic partner. As stated earlier, the most important implication of this work involves contributing to educating human resource professionals into the state-of-the-art issues concerning security and privacy with regard to IoT. Equipped with this knowledge human resource units can move from an operational role to a strategic role within organizations that are looking to innovate using IoTs (Hecklau et al., 2016). As a means to bridge the technical gaps of human resource professionals already identified in the literature, we elaborate each of the specific technical solutions identified in the literature further in the subsections below.

RFID as a Solution

First, we provide our reflections on the RFID as a solution to privacy and security problem in IoT domain. There are three key issues, which mainly impede the widespread adoption of RFID if it were to be used in IoT. The first problem is the expense of the RFID tags. Second, we also need the model tags and readers to ensure highly accurate identification. The third is the incorporation of the RFID into existing IoT systems. Several scientists and researchers are working to introduce low-cost data security and privacy protections to improve applicability (Jia et al., 2012). Several lightweight alternatives have been proposed for RFID, but they are still costly and vulnerable to protection and do not fully address the security issues. Therefore, there is strong research scope for developing an effective ultra-lightweight cryptographic protocol for low-cost RFID systems. Data sharing and secure transfer of objects need to be tackled in this use as well.

Blockchain as a Solution

Second, we discuss the issues concerning blockchain as a solution to privacy and security problem in IoT. With any broadcasts or multi casts required for exchange of keys or certificates, the storage as well as the energy requirements need to be coped with in order to provide a successful implementation

of security and communication protocols for IoT. Resource implementation is one of the biggest challenge with blockchain. A multi-layer network architecture of heterogeneous systems ranging from small low-power devices of sensors to high-end servers needs to be implemented. Initially, the architecture will conform to available infrastructure. It will take decisions on choosing protection frameworks at IoT layers before delivering any services to end users. With heterogeneous networks, architectures and protocols, the IoT paradigm is more vulnerable than any other paradigm to single point of failure. There is also a considerable amount of work to be undertaken to ensure that adequate IoT elements are accessible using this technology.

Fog Computing as a Solution

Third, we discuss mobile fog computing as a solution to privacy and security problem in IoT. By using the function node for data fog computation, light weighted solution is likely (Yi, Hao, et al., 2015). The several small devices associated are the key components of a Fog computing system. These devices are all over the place and help to connect to our surroundings. To maintain this enormous computational environment, there is a need for proper infrastructural facility (Yi, Hao, et al., 2015). Most sensing and actuating devices need a low bandwidth but they can connect a greater number of devices. Existing network communication architectures such as local area network, wide area network, and similar need further exploration in order to improve to the Fog computing system and enable countless IoT devices to rely on this technology. IoT is prone to frequent update and research on fog computing needs to be undertaken so that this infrastructure can handle the need for frequent device updating.

CONCLUSION

The growth of the IoT has not only provided promises to offer new business models and transformational possibilities to many support functions such as human resources with an enterprise, it has also given rise to many security and privacy risks. With more and more people and enterprises using and producing IoT devices, the cyber security threats are also rising. The paper offers a systematic review of the range of IoT specific security and privacy challenges that human resource professional need to comprehend in order to build his technical capability. The paper identifies eight key challenges pertaining to security and privacy with regard to IoT for an enterprise, hence answering the first research objective of the paper. Further, the review answers the second research objective as it also provides key technological possibilities for tackling security and privacy issues which are meaningful to human resource domain as well. We specially analyse three technologies that are promising in this respect: RFID, Blockchain and Fog Computing. We hope this research will enrich both theoretical understanding on the challenges in integrating IoTs into varies business models as well offers a critical overview to the manager involved in digital transformation projects and strategic human resource partners the technical acumen to confidently handle and resolve security and privacy concerned pertaining to use of IoT solutions.

CONFLICT OF INTEREST

The authors of this publication declare there is no conflict of interest.

REFERENCES

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 1–8. doi:10.1109/PRISMS.2014.6970594

Al-Turjman, F. (2020). *Security in IoT-Enabled Spaces*. CRC Press Inc. Retrieved 24 March 2020, from https://www.dawsonera.com/abstract/9780429031915

Alqassem, I., & Svetinovic, D. (2014). A taxonomy of security and privacy requirements for the Internet of Things (IoT). *2014 IEEE International Conference on Industrial Engineering and Engineering Management*, 1244–1248. doi:10.1109/IEEM.2014.7058837

Bag, S., Gupta, S., Kumar, A., & Sivarajah, U. (2021). An integrated artificial intelligence framework for knowledge creation and B2B marketing rational decision making for improving firm performance. *Industrial Marketing Management*, *92*, 178–189. doi:10.1016/j.indmarman.2020.12.001

Bag, S., & Pretorius, J. H. C. (2020). Relationships between industry 4.0, sustainable manufacturing and circular economy: Proposal of a research framework. *The International Journal of Organizational Analysis*. Advance online publication. doi:10.1108/IJOA-04-2020-2120

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, 13–16. doi:10.1145/2342509.2342513

Buyya, R. (2016). *Internet of Things*. Morgan Kaufmann Publishers Inc. Retrieved 2 May 2020, from https://www.dawsonera.com/abstract/9780128093474

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. *Journal of the Association for Information Systems*, *20*(9), 1271–1307. doi:10.17705/1jais.00567

Chen, S. Y., & Macredie, R. (2010). Web-based interaction: A review of three important human factors. *International Journal of Information Management*, *30*(5), 379–387. doi:10.1016/j.ijinfomgt.2010.02.009

Data Center Knowledge. (2016). *IoT Past and Present: The History of IoT, and Where It's Headed Today*. https://www.datacenterknowledge.com/archives/2016/04/29/iot-past-and-present-the-history-of-iot-and-where-its-headed-today

Dhanpat, N., Buthelezi, Z. P., Joe, M. R., Maphela, T. V., & Shongwe, N. (2020). Industry 4.0: The role of human resource professionals. *SA Journal of Human Resource Management*, *18*(1), 1–11. doi:10.4102/sajhrm.v18i0.1302

Fremantle, P., & Scott, P. (2015). *A security survey of middleware for the Internet of Things*. 10.7287/peerj.preprints.1241v1

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016). Holistic approach for human resource management in Industry 4.0. *Procedia CIRP*, *54*, 1–6. doi:10.1016/j.procir.2016.05.102

Hou, X., Li, Y., Chen, M., Wu, D., Jin, D., & Chen, S. (2016). Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures. *IEEE Transactions on Vehicular Technology*, *65*(6), 3860–3873. doi:10.1109/TVT.2016.2532863

IEEE. (n.d.). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Journals & Magazine*. Retrieved 8 June 2020, from https://ieeexplore.ieee.org/document/7005393

Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 1282–1285. doi:10.1109/CECNet.2012.6201508

Juma, M., Monem, A. A., & Shaalan, K. (2020). Hybrid End-to-End VPN Security Approach for Smart IoT Objects. *Journal of Network and Computer Applications*, *158*, 102598. doi:10.1016/j.jnca.2020.102598

Kaupins, G., & Coco, M. (2017). Perceptions of internet-of-things surveillance by human resource managers. *S.A.M. Advanced Management Journal*, *82*(2), 53–64.

Khoo, B. (2011). RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 709–712. doi:10.1109/iThings/CPSCom.2011.83

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Academic Press.

Kraijak, S., & Tuwanut, P. (2015). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, 26–31. doi:10.1109/ICCT.2015.7399787

Krishna, B. V. S., & Gnanasekaran, T. (2017). A systematic study of security issues in Internet-of-Things (IoT). *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 107–111. doi:10.1109/I-SMAC.2017.8058318

Lee, K., Kim, D., Ha, D., Rajput, U., & Oh, H. (2015). On security and privacy issues of fog computing supported Internet of Things environment. *2015 6th International Conference on the Network of the Future (NOF)*, 1–3. doi:10.1109/NOF.2015.7333287

Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D. (2019). Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 9368–9383. doi:10.1109/ACCESS.2018.2890432

Liu, X., Qian, C., Hatcher, W. G., Xu, H., Liao, W., & Yu, W. (2019). Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 79523–79544. doi:10.1109/ACCESS.2019.2920763

Liu, Y., & Zhang, S. (2020). Information security and storage of Internet of Things based on block chains. *Future Generation Computer Systems*, *106*, 296–303. doi:10.1016/j.future.2020.01.023

Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., Boukadi, K., & Maamar, Z. (2017). Privacy-aware in the IoT applications: a systematic literature review. *OTM Confederated International Conferences- On the Move to Meaningful Internet Systems*. doi:10.1007/978-3-319-69462-7_35

Margherita, E. G., & Bua, I. (2021). The Role of Human Resource Practices for the Development of Operator 4.0 in Industry 4.0 Organisations: A Literature Review and a Research Agenda. *Businesses*, *1*(1), 18–33. doi:10.3390/businesses1010002

Metallo, C., Agrifoglio, R., Schiavone, F., & Mueller, J. (2018). Understanding business model in the Internet of Things industry. *Technological Forecasting and Social Change*, *136*, 298–306. doi:10.1016/j.techfore.2018.01.020

Miraz, M. H., Excell, P., Ware, A., Soomro, S., & Ali, M. (2018). *Emerging Technologies in Computing: First International Conference, iCETiC 2018, London, UK, August 23–24, 2018, Proceedings*. Springer.

Nasar, N., Ray, S., Umer, S., & Mohan Pandey, H. (2020). Design and data analytics of electronic human resource management activities through Internet of Things in an organization. *Software, Practice & Experience*.

Oesterreich, T. D., & Teuteberg, F. (2016). Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. *Computers in Industry*, *83*, 121–139. doi:10.1016/j.compind.2016.09.006

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems, 10*(26). http://sprouts.aisnet.org/10-26

Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, *59*(6), 411–423. doi:10.1007/s12599-017-0504-2

Pfaff, O. (2020). *Security for IoT and OT – An Industrial Perspective*. Keynote address to participants of summer school organised by IMT Atlantic, France on "The Future IoT, IoT meets security". https://summerschool20.future-iot.org/program/

Ranger, S. (2020). *What is the IoT? Everything you need to know about the Internet of Things right now*. ZDNet. Retrieved 16 May 2020, from https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework. *Business & Information Systems Engineering*, *59*(6), 385–409. doi:10.1007/s12599-017-0506-0

Rymaszewska, A., Helo, P., & Gunasekaran, A. (2017). IoT powered servitization of manufacturing – an exploratory case study. *International Journal of Production Economics*, *192*, 92–105. doi:10.1016/j.ijpe.2017.02.016

Shamim, S., Cang, S., Yu, H., & Li, Y. (2016). Management approaches for Industry 4.0: A human resource management perspective. *2016 IEEE Congress on Evolutionary Computation (CEC)*. doi:10.1109/CEC.2016.7748365

Shen, C., & Pena-Mora, F. (2018). Blockchain for Cities—A Systematic Literature Review. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 76787–76819. doi:10.1109/ACCESS.2018.2880744

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. doi:10.1016/j.comnet.2014.11.008

Skarmeta, A. F., Hernández-Ramos, J. L., & Moreno, M. V. (2014). A decentralized approach for security and privacy challenges in the Internet of Things. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 67–72. doi:10.1109/WF-IoT.2014.6803122

Strazdins, G., & Wang, H. (2015). Open security and privacy challenges for the Internet of Things. *2015 10th International Conference on Information, Communications and Signal Processing (ICICS)*, 1–4. doi:10.1109/ICICS.2015.7459923

Strohmeier, S. (2007). Research in e-HRM: Review and implications. *Human Resource Management Review*, *17*(1), 19–37. doi:10.1016/j.hrmr.2006.11.002

Strohmeier, S. (2020). Smart HRM–a Delphi study on the application and consequences of the Internet of Things in Human Resource Management. *International Journal of Human Resource Management*, *31*(18), 2289–2318. doi:10.1080/09585192.2018.1443963

Tandalam Aswinikumar, A. (2016). *Bridging cultural discontinuities in global virtual teams: Role of cultural intelligence* (Doctoral dissertation). Paris Saclay.

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). On the Security and Privacy of Internet of Things Architectures and Systems. *2015 International Workshop on Secure Internet of Things (SIoT)*, 49–57. doi:10.1109/SIOT.2015.9

Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169–8181. doi:10.1109/JIOT.2019.2927379

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *29*(3), 129–147. doi:10.1080/12460125.2020.1798591

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. doi:10.1109/JIOT.2017.2694844

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). Fog Computing: Platform and Applications. *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 73–78. doi:10.1109/HotWeb.2015.22

Yi, S., Li, C., & Li, Q. (2015). A Survey of Fog Computing: Concepts, Applications and Issues. *Proceedings of the 2015 Workshop on Mobile Big Data*, 37–42. doi:10.1145/2757384.2757397

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS One*, *11*(10), e0163477. doi:10.1371/journal.pone.0163477 PMID:27695049

Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wireless Communications*, *25*(6), 12–18. doi:10.1109/MWC.2017.1800116

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. doi:10.1109/BigDataCongress.2017.85

Zhu, L. Z. Z. (2017). *Secure and Privacy-Preserving Data Communication in Internet of Things*. Springer. Retrieved 24 March 2020, from https://www.dawsonera.com/abstract/9789811032356

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742. doi:10.1002/sec.795

ENDNOTES

1 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

2 'IoT Past and Present: The History of IoT, and Where It's Headed Today', *Data Center Knowledge*, 2016 <https://www.datacenterknowledge.com/archives/2016/04/29/iot-past-and-present-the-history-of-iot-and-where-its-headed-today>.

Anuragini Shirish is an Associate Professor at Institut Mines-Télécom Business School, France. She hold a master's degree from National University of Singapore and a PhD from University Paris Saclay in France. She is an elected member from her institution for the governance of the LITEM (Laboratoire Innovation Technologies Economie et Management) (EA 7363), a joint research laboratory. She has prior legal work experience in India and Singapore in the domain of corporate and IT laws and is qualified to practice in the courts in India. She has been the academic director of the master's level executive major program called 'Business Information Systems for the Digital Era' and leads the activities of the information systems research team, SMART[2]. Her research focuses on studying the humanistic and instrumental impacts of several socio-technical phenomena in the broad areas of digital work, digital innovation and digital society. Her research has been published in international refereed journals including the European Journal of Information Systems (EJIS), Information Systems Journal (ISJ), Communications of the Association of the Information Systems (CAIS) and International Journal of Information and Management (IJIM). She has also presented her work in several premier IS and management conferences including the International Conference on Information Systems (ICIS), the Academy of Management (AOM), Pacific Asia Conference on Information Systems (PACIS), and the Americas Conference on Information Systems (AMCIS), among others. She has been honoured with several awards including the "Outstanding Educator Award" by the Association for Information Systems (AIS) women's network and the second prize at the Sphinx best thesis award.

Priya Jyoti is a recent graduate of the Masters in Business Information System program 2020 at Institut Mines-Télécom Business School. An experienced Software Developer with a demonstrated history of working in the information technology and services industry. She has presented her work in international conferences. She worked as an apprenti in the technical team within the international unit at Institut Mines-Telecom Business School. She is a certified SAP consultant, having experience working at startups. She is currently working at IBM, Canada. Her research interests include enterprise technology use, the internet of things, security and privacy issues and IT consulting.