UNDERSTANDING THE EFFECT OF IOT ADOPTION ON THE BEHAVIOR OF FIRMS: AN AGENT-BASED MODEL

Riccardo Occa and Francesco Bertolotti

LIUC – Università Catteneo, Corso G. Matteotti 22, Castellanza (VA), Italy

ABSTRACT

In the context of increasing diffusion of technologies related to Industry 4.0 and the Internet of Things in particular, we have developed an agent-based model to simulate the effect of IoT diffusion in companies and verify potential benefits and risks.

The model analyses how firms react to the spread of IoT in the market by analysing its effects on firms' pricing and quality strategies, its impact on variable production costs, and the long-term survival rate of firms.

The model shows how IoT diffusion has the potential to influence the market by supporting both quality and cost improvements.

The results of the model also confirm the potential for significant benefits for businesses, suggesting the opportunity to support the introduction and application of IoT, and clearly show how the use of IoT can be a key strategic choice in competitive market contexts focused on cost strategies to increase business performance and prospects.

KEYWORDS

IoT, agent-based modelling, simulation, adoption, risk, blockchain.

1. INTRODUCTION

The Internet of things has been one of the key components of Industry 4.0 and has seen an increasing spread over the last 10 years. For example, between 2010 and 2017, the number of IoT connections per 100 inhabitants worldwide increased from 2.5 to 14 [1].

The term IoT was first used by Kevin Ashton in 1999 in connection with his work at the Procter & Gamble Company on the potential of RFID [2].

Since then, the interest of the scientific world in the topic of IoT has never ceased. Instead, publications have been explosive growth focusing on IoT issues, exploring its different components, functionalities, and applications. Figure 1 represents the growth of papers that include IoT or the Internet of Things in the title within the SCOPUS database.

David C. Wyld et al. (Eds): EMSA, SEA, AIFU, NLCAI, BDML, BIoT, NCOM, CLOUD, CCSEA, SIPRO - 2022
pp. 207-223, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120619

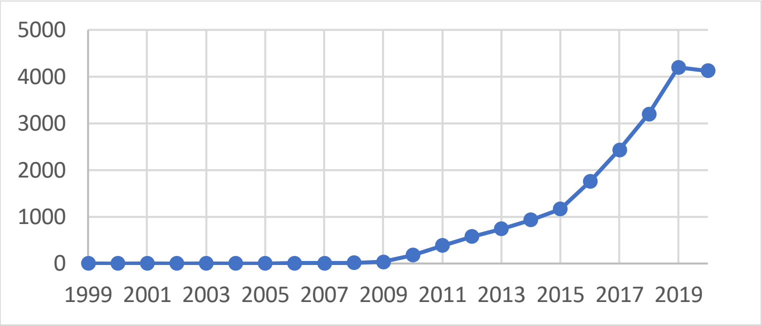

Figure 1. Documents published by year with IoT or Internet of things in the title .Source Scopus database

The scope of the IoT has rapidly expanded beyond manufacturing plants, production, and assembly lines or warehouses, involving many different sectors as shown in figure 2. Among the most widespread applications we can find today:

- Applications related to smart grids and the monitoring and control of electricity transmission generation and consumption systems [3]
- Applications related to the concept of smart cities and smart buildings, equipped with control systems that allow more efficient management of resources, spaces, and the introduction of new services and benefits for the people who live in these places [4]
- The theme of home automation and smart homes, with the possibility, for example, of remotely controlling household appliances and functions in the home [5]
- Smart logistics, with the development of real-time tracking or constant monitoring of product storage characteristics [6]
- Smart mobility, with new services dedicated to the world of the car, such as predictive maintenance and control of vehicle parameters, as well as more precise navigation tools that also allow traffic optimization, leading to autonomous driving [7]
- The development of smart offices, where technology can improve the productivity of the environment and simplify the activities of staff, improving the light and climate conditions of the environment or allowing the introduction of new safety measures.[8]
- The range of services linked to smartphones and wearable devices, which allows applications to monitor one's physical condition or the development of services linked to the habits and behavior of individuals.[9]

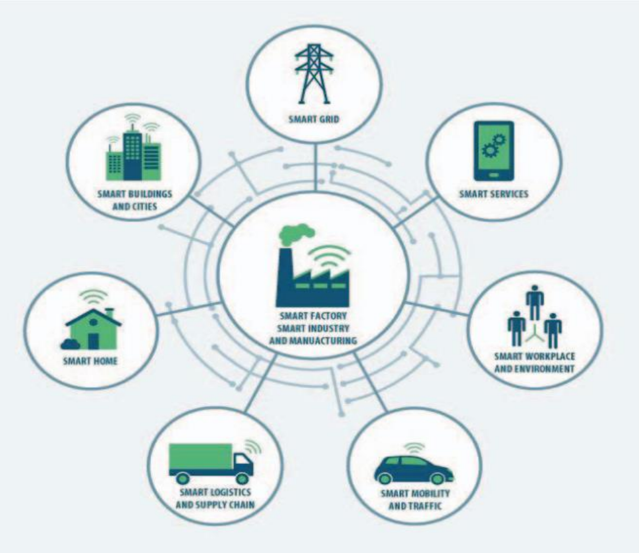
SMART GRID
SMART BUILDINGS AND CITIES
SMART SERVICES
SMART FACTORY SMART INDUSTRY AND MANUACTURING
SMART HOME
SMART WORKPLACE AND ENVIRONMENT
SMART LOGISTICS AND SUPPLY CHAIN
SMART MOBILITY AND TRAFFIC

Figure 2. IoT applications area Source: [2]

IoT has therefore found wide application in manufacturing plants, through the analysis of machinery to enable predictive maintenance, the control of production processes to eliminate defects and waste, the possibility of developing new products and services, and, in general, a greater possibility of controlling and monitoring activities.

However, the introduction of the IoT has also led to the emergence of new risks for businesses, especially of a cyber nature. These risks are linked to several aspects of IoT technologies, including the need to protect and store large amounts of sensitive data and information, the creation of numerous new access points to corporate networks that can be accessed by malicious attackers, and the growth in the dependence of production activities on information and IT systems, which increases the magnitude of damage resulting from their malfunctioning.

Already in 2015, for example, [10] showed that in the previous two years, the growth in the number of connected devices worldwide was followed by an exponential growth in DDoS attacks, measured in bandwidth used.

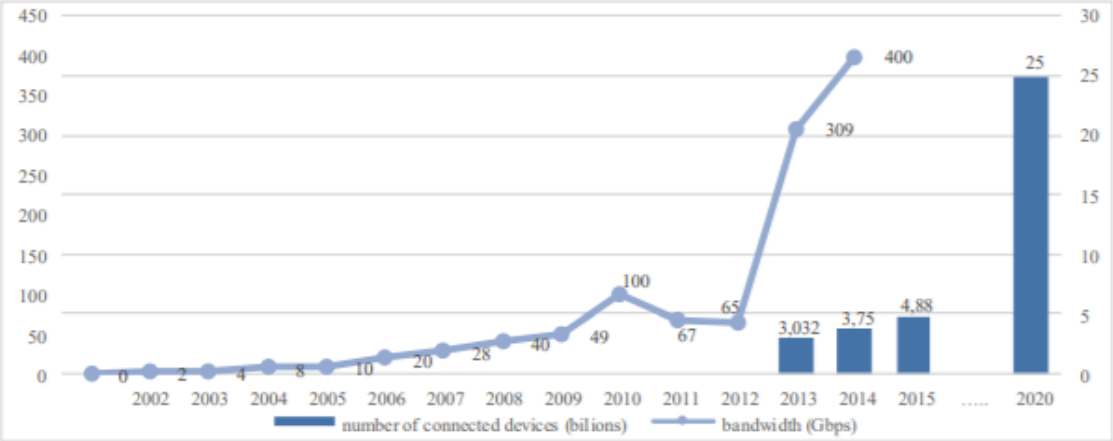

Figure 3. Connected devices and DDOS attack bandwith. Source: [10]

Cyber security risks have been one of the most limiting factors in the spread and adoption of IoT [11]. For this reason, in recent years there has been a lot of research dedicated to solving and mitigating these issues. Among the methods for solving these problems, one of the possible solutions proposed was the adoption of Blockchain technology, resulting in the development of various solutions and proposals that combine the benefits of the two technologies [12].

An agent-based modeling (ABM) was developed to study these phenomena. ABM is a simulation technique in which a system is modelled by creating an assortment of autonomous decision-making entities which stands for the entity of the modelled system [13]. While an ABM is not the only available technique, but it is well fitted to model and simulate complex systems in which individuals take heterogeneous decisions following rules and observe the macro behavior of the system.

This work presents a simple agent-based model of a market of productive firms, in which each company competes. Firms have a given cost structure and can vary their strategies, to increase or decrease the quality and the price of the product. Each firm has the possibility to invest in the adoption of IoT technology, which can reduce the variable cost of production (e.g., higher efficiency), but allows for IoT attacks. Consequently, the decision implies a given amount of uncertainty, an expected benefit, and potential damages.

The purpose of the model is twofold. On the one side, it attempts to investigate the relationship between the IoT risk conditions, and the strategies adopted by firms. On the other, it finds a relationship between the adoption of IoT and the probability of survival in the market, especially when the market prefers low-cost products to high quality ones.

The structure of the paper will proceed as follows:

- section 2 will describe the current state of IoT technologies, with a focus on adoption and deployment and the characteristics of the Industrial Internet of Things. The security issues of IoT will then be presented.
- Section 3 will describe the characteristics of the agent based model adopted. The mathematical relations at the base will be presented and the assumptions of the simulations will be explained.
- Sections 4 and 5 will show the results obtained from the model and the discussions and conclusions derived from them.
- Section 6 will include proposals for future developments and additions to the proposed model.

2. BACKGROUND

2.1. IoT Adoption and Diffusion

As mentioned above, the growth of the IoT in recent years has been remarkable, However, this growth has not always been uniform across countries or economic sectors, and sometimes different applications have shown different peculiarities and characteristics.

Looking at Table 1, we can see that the number of IoT connections varies in different countries, with a higher diffusion in the EU, USA, and China than in other areas of the world.

Table 1. IoT connections per 100 inhabitants in different countries. Source: [1]

Country	2010	2011	2012	2013	2014	2015	2016	2017
China	0.8	1.4	2.4	3.6	4.9	7.3	12.2	24.0
France	4.1	5.5	7.3	10.6	12.6	16.0	17.1	22.5
Germany	2.9	3.7	4.9	6.4	8.4	11.2	13.7	16.6
Japan	3.4	4.7	6.1	7.2	8.9	10.1	12.1	13.8
Sweden	24.1	31.8	41.3	53.7	63.2	68.8	88.0	105.8
United Kingdom	5.0	6.4	7.9	8.7	10.4	12.4	15.3	17.6
United States	5.8	7.6	9.4	11.6	13.9	17.3	21.0	27.5
EU countries	4.9	8.7	11.5	14.3	16.9	19.6	23.3	27.7
OECD countries	4.9	8.0	10.4	12.9	15.3	17.8	21.2	25.4
Non-OECD c.	0.6	1.0	1.5	2.0	2.6	3.2	4.1	5.2
All countries	2.5	4.1	5.4	6.7	8.1	9.6	11.5	14.0

However, even within these areas, we can find differences.

If we look at the data on IoT adoption in businesses in Italy, [14] we can see that in 2019 73% of large companies will have started IoT-related projects, compared to 29% of SMEs.

However, in Germany, studies such as [15] have shown that company size is not a factor in IoT adoption.

Some countries have specificities related to the different levels of infrastructure available, e.g. in India, one of the main determinants of IoT adoption is the availability of adequate Internet connections [16].

However, numerous studies and analyses have made it possible to observe certain basic limitation factors common in different sectors or countries. These limiting factors include privacy and security issues, lack of defined standards, and issues related to lack of organizational support [17][18].

A final element to consider regarding factors that may limit the adoption of IoT is the cost of implementation. There is no clear position in the scientific world about the actual impact of costs in IoT adoption.

Some studies, such as [19], do not believe that the cost of implementing IoT technology is a relevant factor in influencing the adoption rate. Other studies, however, such as [20], have identified cost as a limiting factor, especially in SMEs.

2.2. The Industrial Internet of Things

The applications of the Industrial Internet of Things are varied and strongly influenced by the sector in which different industries operate and their supply chains.

IIoT in companies is generally able to lead to significant performance gains. At a general level, [1] has shown that within a country or an increase in IoT device connections corresponds to an increase in total factor productivity (TFP).

At the individual enterprise and application level, productivity gains are found in several IIoT applications.

The use of IoT for the introduction of IoT and Edge Computing-based Manufacturing, for example, allows for the development of decentralized mass production models, where the reduced operation completion time required allows for an increase in operational performance resulting in increased productivity [21].

Another area of application is monitoring and control, where the ability to track data at every point in production, including storage parameters during transport activities, allows for a minimization of waste and a reduction in the time required for machine and product control activities [21]. Monitoring can also be used to introduce predictive maintenance mechanisms to optimize plant and machinery set-ups and limit the occurrence of faults and waste in production. It should also not be overlooked that the systematic collection and analysis of production data can be the basis for the development of further simulations and analyses for the introduction of further productions or for the introduction of innovations aimed at improving existing productions [22].

Two other areas of IoT application that can often be found together are robotics and localization. Concerning industrial robots, in addition to the aforementioned issue of predictive maintenance, which can also be applied here, a new possibility opened up by the use of IoT is that of reactive replanning. The introduction of robots in production entails the development of more dynamic and reactive environments, which increases productivity but also increases the risk of errors or accidents when a predetermined action of a robot collides with a different situation or unexpected human behavior. Reactive replanning allows, thanks to the constant analysis of movements and the introduction of an automatic supervision mechanism, to react to unforeseen situations, or to modify the behavior of the machines in a new pattern more efficiently than the previous one when the opportunity arises. This makes it possible to increase safety and optimize the operation of the production system [23].

The localization of robots is an active part of this process, but it also finds great application in the automation of tasks performed by moving automatic components. A classic example is Amazon's Kiva robots, used in the handling of goods in warehouses, which enable major performance improvements, with cases of up to 50% more goods being stored in the same space and significant gains in efficiency [24].

2.3. The IoT Security Risks

When talking about IoT cybersecurity issues or naming cyber-attacks, we are not referring to a single issue that needs to be addressed. There are many different types of actions that can damage an IoT system or its user.

[25] have proposed the classification of threats shown in Figure 4, which distinguishes the risks into 4 different types; these categories are found in most of the proposed classifications:

Physical attacks: involve a reduction in the capacity of a network of IoT systems or part of it, usually requiring proximity to the systems by the implementer. The consequences of these attacks can include battery depletion, with the consequent inability to continue activities, as in sleep denial attacks, or the theft of information, as in the case of fake node injection or side-channel attacks, or the interruption of network operation, as in tampering or permanent denial of service [25] [26]. Another possible source of this type of attack can be the ones based on social engineering techniques, which involve manipulating users to obtain sensitive information or access the network [26].

Network attacks: involve using the IoT network to create damage. Here again, the purposes can be varied, from intercepting sensitive information (sinkhole or man in the middle attacks) to altering or deleting data and information (spoofing or unauthorized access), to disabling the network or part of it (routing information attacks or Distributed Denial of Service attacks) [25][26].

Software attacks: are based on the use of software, Trojans, or malware to overcome the protective measures of IoT networks and gain access to information or the ability to modify and delete data. The targets of these attacks may include reaching and infecting elements such as data centers and cloud centers [25] [26].

Data attacks: relate to three types of cyber damage, data manipulation in data centers, unauthorized access to data centers and unauthorized disclosure and dissemination of personal data [25].

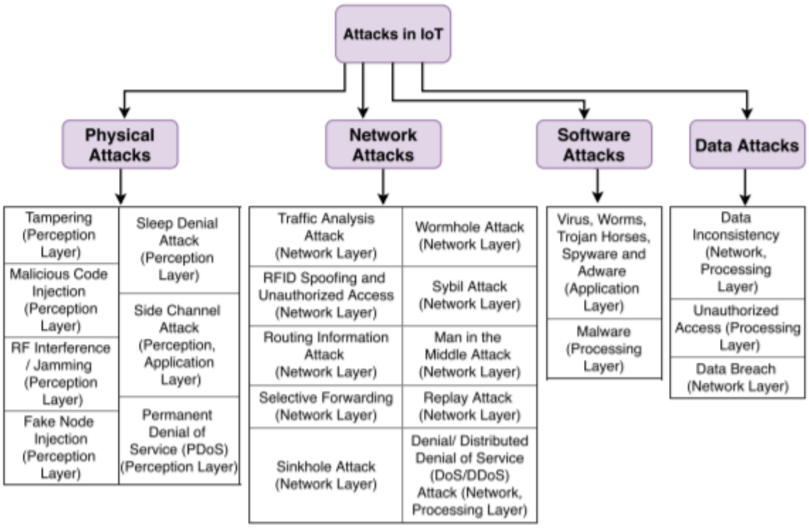
Attacks in IoT
Physical Attacks
Network Attacks
Software Attacks
Data Attacks
Tampering (Perception Layer)
Malicious Code Injection (Perception Layer)
RF Interference / Jamming (Perception Layer)
Fake Node Injection (Perception Layer)
Sleep Denial Attack (Perception Layer)
Side Channel Attack (Perception, Application Layer)
Permanent Denial of Service (PDoS) (Perception Layer)
Traffic Analysis Attack (Network Layer)
RFID Spoofing and Unauthorized Access (Network Layer)
Routing Information Attack (Network Layer)
Selective Forwarding (Network Layer)
Sinkhole Attack (Network Layer)
Wormhole Attack (Network Layer)
Sybil Attack (Network Layer)
Man in the Middle Attack (Network Layer)
Replay Attack (Network Layer)
Denial/ Distributed Denial of Service (DoS/DDoS) Attack (Network, Processing Layer)
Virus, Worms, Trojan Horses, Spyware and Adware (Application Layer)
Malware (Processing Layer)
Data Inconsistency (Network, Processing Layer)
Unauthorized Access (Processing Layer)
Data Breach (Network Layer)

Figure 4. IoT security attacks classification Source: [25]

Different types of cyber-attacks require different and specific countermeasures. In addition to specific solutions, however, the growth of the IoT has stimulated the search for models and architectures that can resist different types of threats more effectively [27] [28]

Among these architectures, several are based on blockchain technology, which thanks to several of its characteristics such as the non-repudiation of transactions, decentralization, or the difficulty of modifying the transactions entered promises to provide better performance in terms of security [29].

Blockchain architectures for IoT are often multi-layer architectures because the use of blockchain can be costly in terms of energy and computing power. To this purpose, proposals envisage the use of "regional" nodes [30], which transfer the most onerous tasks to a smaller number of dedicated components, in order to guarantee normal performance for the sensors and elements that compose the IoT infrastructure.

Other architectures focus on particular aspects or processes related to IoT networks, [31] for example proposes a blockchain architecture to manage authorizations and access and ciphration keys. These are just a few examples of the many models developed and proposed.

3. AGENT-BASED MODEL

3.1. Model Description

We introduce here the model underlying the simulation results displayed in the succeeding section. The model has an exploratory intent. Consequently, we used a few simplifications. This was necessary for a twofold reason. Firstly, the more abstract is the model, the more general could be the results. Secondly, we aim at identifying and study a single phenomenon. A simpler model could be more suited to address the causal effect of a parameter variation connected to the IoT effect.

In the model, there is a single breed of agents, the firms. Firms can take two kinds of actions: they can operate on the market, or they can perform investments in IoT. Firms cannot communicate with each other, they only interact indirectly through their interactions with the market and their results. Consequently, the topology of the ABM can be described as a star network, with a single central entity (the market) with whom the agents interact. The dynamic of the market is very simple. Especially, we supposed that firms are homogeneous related to their size, produce and sell only one kind of product and their confirms are supposed to have only two kinds of costs: fixed costs and variable costs. Fixed costs are the same for each firm, and do not change in time. Variable costs depend linearly on three elements: the quality of the produced product, the number of products sold, and the efficiency of the production process, moderated by the level of adoption of IoT technologies and their influence on the variable costs. Mathematically, they are defined as:

$$vc = q \cdot c\_q \cdot (1 - e) \cdot (1 - i_i \cdot i_s)$$

with vc variable cost of production, q product quality, c_q cost of quality, e efficiency of the production process, i_i IoT technologies adoption, and i_s IoT technologies savings.

Therefore, a firm is sustainable only when the difference between turnover and variable cost is greater than fixed costs. Hence, a successful strategy is any strategy that allows a firm to obtain this target. A strategy is made by a couple of elements: product price and product quality. In the model, it is assumed that both can be changed at any time. Moreover, in the market, a product is sold in a single distribution channel at the same price.

At each time step, the market has a certain demand for the product sold by the modelled firm. The total demand is sampled at each time step from a random normal distribution with a fixed mean and variance. The unity of measure of the demand is the amount of goods that the market requires. After the demand is generated, an allocation process takes place. First, all the quality and prices of each firm are collected and normalized. The prices are normalized inversely so that the minimum price corresponded to the value 1 and the maximum price with the value 0. It models the preference of customers for cheaper products. Second, a product success index is computed as follows:

$$\mathrm{psi} = q_n \cdot \mathrm{pm} + p_n \cdot (1 - \mathrm{pm})$$

with psi product success index, q_n normalized quality, p_n normalized price and pm preference of the market (0 if it considers only price, 1 otherwise).This formula has two implications. First, higher normalized values of price and quality can bring to higher product success index. Second, the final value depends on the specific features of the simulated market. The market share of each firm $i$at each time step is allocated according to the following rule:

$$ms_i = \frac{\mathrm{psi}_i}{\sum_i \mathrm{psi}_i}$$

This allocation process is possible only assuming that every customer can purchase the product, and there are not any logistic limitations.

The decision making of agents is simple. While competing in the market, firms can perform two actions: the production (and automatically selling) of products and the change of strategy. The production level at each time step coincides with the demands coming from the market to the specific firms. In the model, no firm has a production capacity limitation, and the presence of time delay between the production moment and the availability of a product on the market is ignored because we considered these two factors not relevant for the risk preference adaptation of firms regarding IoT risks. In this first phase, the cash level of a firm is updated according to the profit. If the profit is positive, the cash level increases; otherwise, it decreases. If the cash level of a firm goes to 0, the firm fails, and it is removed from the simulation. Regarding the definition of strategies, agents behave naively towards the market, and they do not have any assumption related to the reason why a strategy is successful or not. When an agent is having a negative result (e.g., a negative profit) for more than a certain amount of time steps (defined by a parameter), it can change strategy while picking a new couple of product quality and product price at the same time. The new values are sampled from a random continuous uniform distribution. The changing in pricing strategy does not directly affect the cost of the product but the value of the markup, which affects the selling price as the following equation describes:

$$\mathrm{p} = \mathrm{c} \cdot (1 + \mathrm{m} \cdot \mu)$$

with p product price, c product cost, m markup and μ price strategy.

In this model, firms can decide or not to adopt an IoT technology into their production process. The effect of the introduction of IoT relates to production efficiency. The IoT level of a firm is defined by a real number between 0 and 1. The higher is the IoT level of a firm, the lower are the variable cost of production of a product. It means that it will be more easily sustainable (because of the lower variable costs) and more successful on the market (because a reduction in the production costs implies a reduction of the selling price, which is computed with a markup). So, the level of the benefit is regulated by a specific parameter. Nevertheless, implementing IoT makes it possible to be a target of IoT attacks. The effect of an IoT attack is to take from the firm a given amount of money, reducing the cash level. The amount of money is computed sampling from a power law distribution, which exponent is a parameter of the model. The sampled value (between 0 and 1) is later multiplied for the last turnover of the firm, to give the appropriate magnitude to the IoT issue, because in real-world the monetary cost of an attack is related to the size of a firm. Hence, a firm can decide to invest or not in IoT technologies, according to their IoT adoption inclination, which stands for their profile of risk. The higher is their inclination, the more likely is for a firm to invest in IoT technology.

The scheduling of the model proceeds as follows. First, the agents' list is shuffled, so that the order in which firms are called changes at each simulation. Second, each agent updates the quality and the selling price (which derives from the production cost) according to their strategy.

So, if in the previous time step the strategy did not change, quality and selling price remains the same. Third, the market allocates the demand to different firms, and their financial status is updated with the profit. Fourth, the model removes the firms with a cash level below 0. Fifth, if firms had a negative performance in terms of profit in the last periods (the exact number is a parameter of the model) and did not change the strategy recently (as well, the minimum number of periods between two changes is a parameter of the model), it can change strategy with a given probability. Sixth, firms can invest or not in IoT technologies. Finally, firms that employ IoT technologies can experience informatic attacks. Figure 5 shows the scheduling of the model.

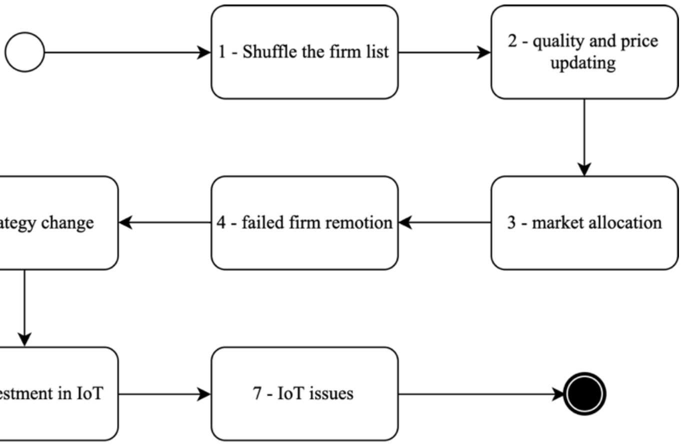

Figure 5. Scheduling of proposed model

The model is developed using Python 3.8 as programming language, without employing any specific framework for agent-based modelling, in an Anaconda environment.

3.2. Model Exploration

The results are achieved by simulating the model 20’000 times, variating the parameters. The purpose of this methodology, called grid sampling, is to identify the effect of each parameter on the outcomes, and consequently identify some specific relationships between the operating conditions and the outcome of the model. Under this point of view, it is possible to describe the model exploration as a black box. The inputs are the parameters variation, while the output the resulting values of the model. Figure 6 describes it.

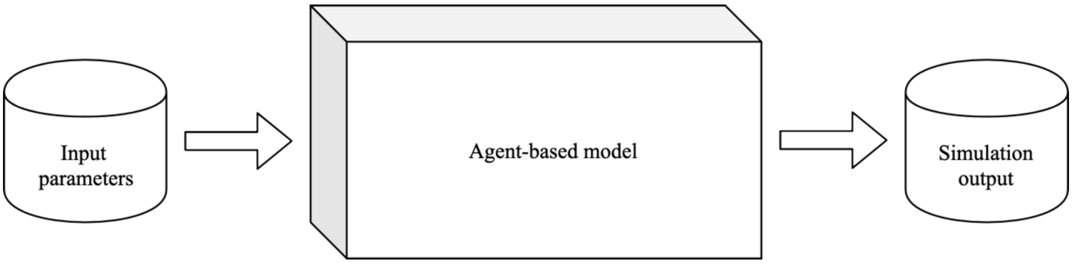

Figure 6. Black box concept application in the model

The parameters shuffled during the grid sampling are observed in Table 2, while Table 3 resumes the outcome of the simulation, that we employed to analyze the results.

Table 1. Parameter shuffled during simulations

Parameters	Meaning
init_firms	Number of initial firms in the market
pref_mkt	Preference of the market in terms of quality or price
cf_act	Fixed costs of activity of firms
q_cost	Variable cost for each unity of quality of the product
max_mkup	Maximum markup (price on production cost)
IoT_ar	Adoption rate of IoT technologies (speed of implementation)
IoT_sv	Saving on variable costs with IoT technology
IoT_iss_fq	Frequency of issues related to the adoption of IoT technology
IoT_iss_mn	Mean of issues (% of turnover) related to the adoption of IoT technology
IoT_iss_ex	Exponent of issue (power law) related to the adoption of IoT technology

Table 2. Simulation's outcomes

Output	Meaning
mean_IOT_adop	Mean level of adoption of IoT technologies
mean_IoT_incl_fail	Mean level of adoption of IoT technologies in failed firms
mean_IoT_incl_survived	Mean level of adoption of IoT technologies in surviving firms
mean_q	Mean quality strategy of survived firms
mean_mu	Mean price strategy of surviving firms
pct_firms_survived	Share of initial firms that survived
num_IoT_issues	Number of IoT issues
mean_IoT_Issues	Mean impact of IoT issues

The simulation results are analyzed using Python 3.8, on an Anaconda environment.

4. RESULTS

This section divides as follows. Firstly, the effect of the benefit of IoT on firms' strategies is shown. Secondly, the relationship between the IoT risk and the rate of survival of firms at the end of the simulation is investigated. The last part illustrates the effect of the parameters on the difference in risk preferences related to the adoption of IoT technologies between surviving and not surviving firms.

4.1. Firms' Strategies

This section investigates some notable relationships between environmental conditions and firm strategies that appeared in the simulation dataset. These results are computed by observing the behavior of the mean of a dependent variable on a dependent variable, employing a simple 2D plot.

Figure 7 and Figure 8 respectively show the relationship between the mean price and quality strategy of the firms that survived in the model, and the way it was affected by the effect of the introduction of IoT technology on the variable cost reduction.

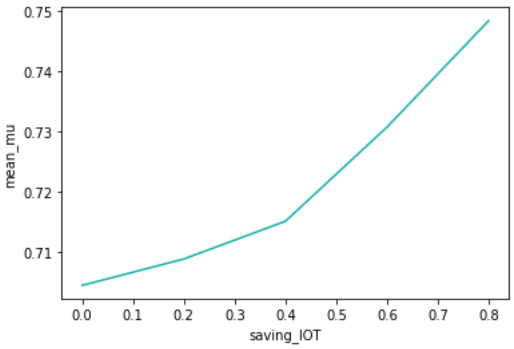

Figure 7. Firm's mean price and quality strategy

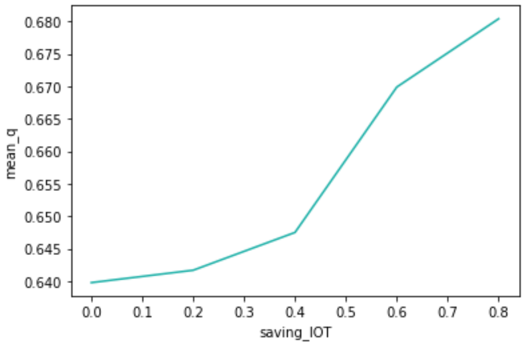

Figure 8. Firm's mean price and quality strategy in presence of IoT

Figures show that it exists a growing relationship between the quality and price strategies (axis of ordinates) and the variable costs reduction related to the IoT (abscissa axis). At a first sight, this result seemed contradictory. Since a firm should hypothetically focus on price or quality, we expected at least one of the relationships to be inversed. Nevertheless, we found two potential explanations for this phenomenon. First, the higher was the effect of IoT on the costs, the more likely were for firms to survive if they adopted a price strategy, that could be more competitive (because of the increase in the margins). Second, the savings in the variable costs affected the price adopted by the firm, because of the markup strategy. It implied that the higher was the savings due to IoT, the more profitable would be a firm on the market, and consequently the more profitable was a quality strategy. Since the results in Figure 8were computed only on firms that survived at the end of the simulation, it became logical that the positive effect of IoT improved the fitness of a quality strategy in that specific competition environment.

4.2. Iot Risk and Firm Survival

This section investigates the effect of IoT inclination on the probability of survival of firms. Specifically, we investigated the mean IoT inclinations of firms that survive and the connection between the number of IoT issues and the share of firms that survived until the end related to the risk connected to the IoT. Logically, the higher the risk of IoT attack, the higher the risk of implementation of IoT technologies. We observed that this is a non-linear relationship. More precisely, the number of issues related to IoT technologies increases with the share of firms surviving, but they decrease after reaching a peak. Figure 9 displays this connection.

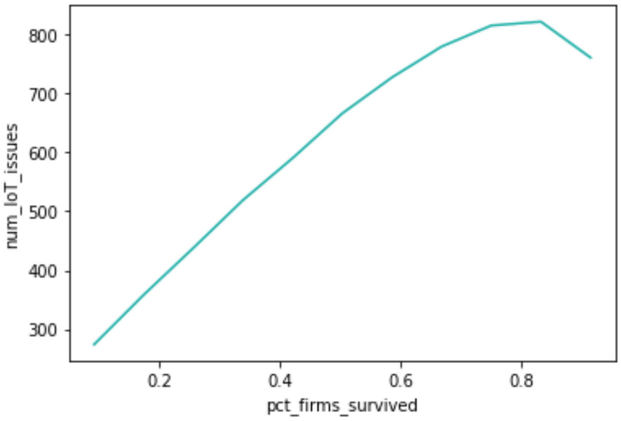

Figure 9. Shares of surviving firms and IoT issues occurring

We explain this phenomenon as the result of two concurring strengths. On the one side, the more firms survived, the more firms can implement IoT technologies. Consequently, the number of IoT issues increases. Nevertheless, after a given threshold, the market context is such that also allows firms that do not implement IoT technologies to survive. Consequently, the total number of issues in the simulation is below the peak value.

4.3. Difference in IoT Adoption Inclinations between Surviving and not Surviving Firms

In this paragraph, we investigate the difference between the mean IoT adoption inclination of survived firms and the mean IoT adoption inclination of failed firms. This value was computed for each resulting simulation, and for simplicity, we refer to it as "*difference*". The values of the difference in the sampling were distributed as it is shown in Figure 10.

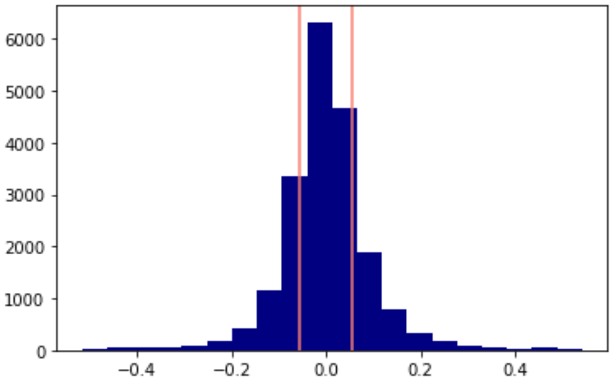

Figure 10. "difference" distribution at the end of simulations

We identified two notable groups of simulations. We called "*over*" the samplings in which the value of the difference is above the 80th percentile, and "*under*" the samplings in which the value of the difference is above the 20th percentile. In figure 10, these are represented by the two vertical lines. In this way, we could isolate two groups in which the difference of inclination affected the rate of survival, both positive and negative.

Figure 11 provides an overview of the effect of IoT adoption inclination on the overall success of firms.

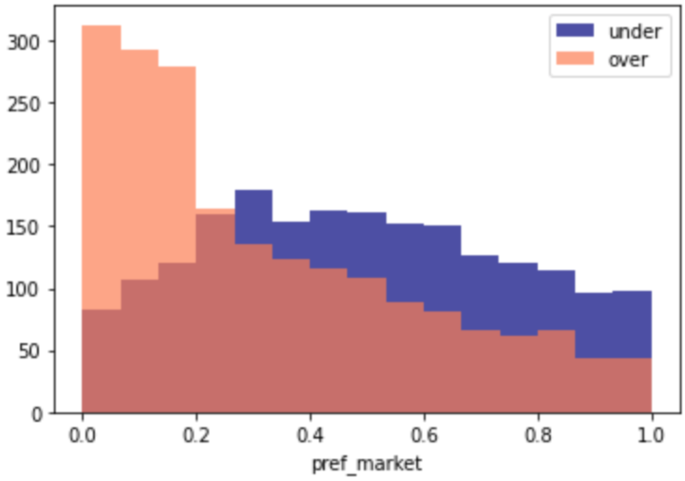

Figure 11 IoT adoption and success rate of firms

Figure 11 displays the distribution of market preferences for simulations in which firms have high and low *difference*. It is observable that the distributions had different shapes and different moments. More precisely, the *under* sampling had a mounded market preference distribution, while the *over* sampling had a j-shaped distribution, which resembled a power law distribution. The overlapping of the distributions showed that when the market strongly preferred the quality over the price, the competition process selected more likely firms with higher preferences in adopting IoT technologies.

We interpreted this phenomenon as the consequence of the lower production costs connected to the adoption of IoT technologies gives higher market shares to firms that invested in IoT. This market share grew progressively with the decrease of the parameter *market preferences* (when the relevance of price for costumers' decision increased). Therefore, the profit increased, and with it the probability of not failing.

5. Discussion and Conclusions

If we look at the results of the model in search of possible practical implications, the first result to consider is the positive influence that the introduction of IoT brings both to applications of cost leadership strategies and to those focused more on increasing the quality of the offer (figure 7 and 8). This allows us to consider as positive and desirable the effects of a high diffusion of IoT in enterprises, and suggests that it is desirable to search for initiatives and policies that favour its diffusion.

A second aspect that should not be underestimated is the particular success that the IoT seems to have in markets characterised by price competition. A success that manifests itself in increase of competitivity in firms adopting the IoT than others. In these contexts, support for the introduction of IoT technologies could therefore be a precise strategy for both economic and political entities interested in supporting and guaranteeing greater success of their productive sectors in contexts of strong competition on production costs and sales prices that are common in the context of international globalisation where many companies operate today.

However, there are also elements to pay attention to. Figure 9 shows that in a context of wider firms survival and wider spread of IoT, the number of attacks and cybercrimes increases.

Although this does not seem to lead to a reduction in the number of surviving enterprises, it could lead to a reduction in market profit. It would therefore be necessary to look for methods and solutions to mitigate the occurrence of these cyber-attacks.

6. FUTURE DEVELOPMENTS

The model proposed in this paper can be used as a basis for various future implementations. A first hypothesized extension is the possibility of obtaining a more precise estimation of risk preferences by companies through the use of a dedicated questionnaire that would allow for detailed profiling of real cases and actors. Starting from this data, it would be possible to obtain a greater definition of the results previously shown, with the possibility of defining them within specific economic sectors or territorial areas. It would also then be possible to analyse how the actual adoption of the IoT by businesses could vary as the risk associated with the introduction of the IoT changes.

Furthermore, it could be possible to implement a similar model introducing a “criminal” agent, which could or could not invest in IoT technology, and then assess if there are some interesting co-adaptation dynamics in the risk preferences of firms. Finally, it could be possible to investigate if the results of this model would change with different conditions. For example, if an increase of uncertainty given by demand with a given trend or seasonality would increase or decrease the resulting risk preferences of firms related to the adoption of IoT.

Further simulations related to the possibility of simulating the results of policies favorable to the introduction of the IoT in competitive markets could also be included, to verify whether they could be used as a tool for promoting or protecting an economic system by both economic and political entities.

In the future, it would be desirable to hypothesize possible impact analyses of specific IoT architectures and projects dedicated to specific economic sectors modelled based on real market parameters in order to realistically simulate the benefits that can be hypothesized from the proposed innovations and to allow the related opportunities to be fully assessed.

REFERENCES

[1] Edquist, H., Goodridge, P. and Haskel, J., 2019. The Internet of Things and economic growth in a panel of countries. Economics of Innovation and New Technology, 30(3), pp.262-283.

[2] Al-Sarawi, Shadi, et al. "Internet of Things market analysis forecasts, 2020–2030." 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE, 2020.

[3] Siozios, K., Anagnostos, D., Soudris, D. and Kosmatopoulos, E. IoT for Smart Grids.

[4] Giang, N. K., Lea, R., Blackstock, M., & Leung, V. C. (2016, December). On building smart city IoT applications: a coordination-based perspective. In Proceedings of the 2nd International Workshop on Smart (pp. 1-6).

[5] Govindraj, V., Sathiyanarayanan, M., & Abubakar, B. (2017, August). Customary homes to smart homes using Internet of Things (IoT) and mobile application. In 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon) (pp. 1059-1063). IEEE.

[6] Song, Y., Yu, F. R., Zhou, L., Yang, X., & He, Z. (2020). Applications of the Internet of things (IoT) in smart logistics: A comprehensive survey. IEEE Internet of Things Journal.

[7] Porru, S., Misso, F. E., Pani, F. E., & Repetto, C. (2020). Smart mobility and public transport: Opportunities and challenges in rural and urban areas. Journal of traffic and transportation engineering (English edition), 7(1), 88-97.

[8] Furdik, K., Lukac, G., Sabol, T., & Kostelnik, P. (2013). The network architecture designed for an adaptable IoT-based smart office solution. International Journal of Computer Networks and Communications Security, 1(6), 216-224.

[9] Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey. IEEE Access, 8, 69200-69211.

[10] Peraković, D., Periša, M., & Cvitić, I. (2015). Analysis of the IoT impact on volume of DDoS attacks. XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionomsaobraćaju–PosTel, 2015, 295-304.

[11] Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1577-1581). Ieee.

[12] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184-1195.

[13] Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. Proceedings of the national academy of sciences, 99(suppl 3), 7280-7287.

[14] Osservatori.net. 2021. Buon compleanno Internet (of Things). [online] Available at: <https://www.osservatori.net/it/eventi/on-demand/convegni/buon-compleanno-internet-of-things>.

[15] Arnold, C., & Voigt, K. I. (2019). Determinants of industrial internet of things adoption in German manufacturing companies. International Journal of Innovation and Technology Management, 16(06), 1950038.

[16] Luthra, S., Garg, D., Mangla, S. K., & Berwal, Y. P. S. (2018). Analyzing challenges to Internet of Things (IoT) adoption and diffusion: An Indian context. Procedia Computer Science, 125, 733-739.

[17] Carcary, M., Maccani, G., Doherty, E., & Conway, G. (2018, September). Exploring the determinants of IoT adoption: Findings from a systematic literature review. In International Conference on Business Informatics Research (pp. 113-125). Springer, Cham.

[18] Bilgeri, D., & Wortmann, F. (2017). Barriers to IoT business model innovation.

[19] Mącik, R. (2017). The adoption of the internet of things by young consumers–an empirical investigation. Economic and Environmental Studies, 17(2 (42)), 363-388.

[20] Tu, M. (2018). An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management: A mixed research approach. The International Journal of Logistics Management.

[21] Chalapathi, G. S. S., Chamola, V., Vaish, A., & Buyya, R. (2021). Industrial internet of things (iiot) applications of edge and fog computing: A review and future directions. Fog/Edge Computing For Security, Privacy, and Applications, 293-325.

[22] Ayvaz, S., & Alpay, K. (2021). Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. Expert Systems with Applications, 173, 114598.

[23] Lager, A., Papadopoulos, A., & Nolte, T. (2020, September). IoT and Fog Analytics for Industrial Robot Applications. In 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (Vol. 1, pp. 1297-1300). IEEE.

[24] Yudiansyah, A., Keke, Y., & Veronica, V. (2020). CAN THE MOBILE ROBOT BE A FUTURE ORDER-PICKING SOLUTION?: A CASE STUDY AT AMAZON FULFILLMENT CENTER. Advances in Transportation and Logistics Research, 3, 800-806.

[25] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, 102481.

[26] Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 32-37). IEEE.

[27] Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In Digital twin technologies and smart cities (pp. 123-149). Springer, Cham.

[28] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.

[29] Kshetri, N. (2017). Can blockchain strengthen the internet of things?. IT professional, 19(4), 68-72.

[30] Bao, Z., Shi, W., He, D., & Chood, K. K. R. (2018). IoTChain: A three-tier blockchain-based IoT security architecture. arXiv preprint arXiv:1806.02008.

[31] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., ... & Zanichelli, F. (2018, April). IoT Chain: A blockchain security architecture for the Internet of Things. In 2018 IEEE wireless communications and networking conference (WCNC) (pp. 1-6). IEEE.

AUTHORS

Francesco Bertolotti

I'm a industrial engineer and PhD candidate at LIUC university, currently visiting at the TU/e. My field of expertise is the simulation of risk preferences adaptation in socio-economical systems, especially employing agent-based modelling. I am member of the Complex System Society.

Riccardo Occa

I'm a industrial engineer and PhD candidate at LIUC university. My field of expertise is Logistic and Supply Chain 4.0, with a particular focus on IoT and Blockchain technologies.