Internet of Things: Financial Perspective and Associated Security Concerns

Bilal Ahmad Pandow, Alwi M Bamhdi, and Faheem Masoodi

***Abstract*—The internet of things (IoT) has grown at a significant pace and has revolutionized the whole technological aspects of internet and things. In the paper around 800 IoT companies headquartered in various countries globally were analyzed. It was observed that the financial returns of select IoT companies for past five years have witnessed a decent growth however; the industry witnessed a slight dip in the year 2016. Appropriate privacy and security measures need to be in place to effectively secure the communications and storage of huge amounts of data generated.**

***Index Terms*—Internet, finance, IoT, security.**

I. Introduction

The term Internet of Things (IoT) encompasses a set of heterogeneous connected devices that are connected via some communication protocols and sensors, which enable us to locate, identify and operate upon these devices.

In simpler terms and as can be seen in the cf. Fig. 1 we can say it is the network of physical things, devices, automobiles, constructions and many other physical objects which are implanted with microelectronics, software, antennas, and are connected with network that enables these things to gather and interchange data. The linkage of physical-things to the Internet makes it conceivable to have the access to a remote sensor-data which will allow the control for the physical-world from quite a distance. The reduction of cost, energy consumption and size of hardware devices which are meticulously linked to each-other, in the present day it allows the manufacturers to produce exceedingly small and economical low-end processors [1].

The latest IoT trends in the business suggest that the companies should invest more ensuring R&D and bring products quickly in the market while safeguarding the privacy of users. The companies also should focus on producing the IoT products which are of ease to the users, so that the end-users can maximize the benefits by employing the IoT products. Also, the firms should developing robust IoT-standards that would make it possible to minimize the insecurity and boost new firms to enter the market [2]

Given the significance of IoT and the growth it has achieved over the years, it is important to study the financial growth that IoT companies have accomplished. Also, to compare other technological firms so as to link the growth within the same industry.

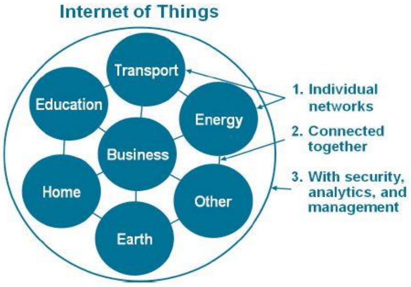

Fig. 1. The Internet of Things network; source: Cisco IBSG.

There have studies which have estimated that about 555 billion units in an Auto-ID Center-specific things will have selection in the supply chains [3]. While in the near future there will be many IT-enabled things surrounding us where people will be either directly or indirectly communicate with these things also, what will be required is a new updated network infrastructure, that will enable the IOT at a large scale.

Besides, having a look at the internet users in the world by region, it wouldn't astonish most that 49% of the users are from Asia, followed by Europe at 16% and Africa at 11%, further regional details can been seen in cf. Fig. 2. The firms dealing with IoT at all levels have to have their focus in the Asian region as almost 50% users are from this region.

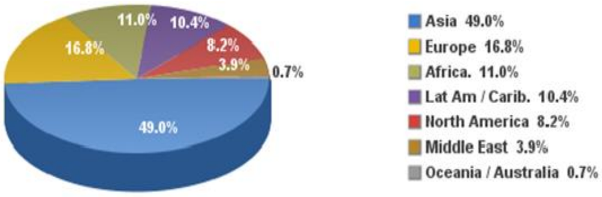

Fig. 2. Internet users in the world by region; source: Internet world stats as on June 30, 2018.

As of today, there are multiple challenges faced by IOT in terms of constrained physical capabilities, standardization, architecture, privacy and security. Considering the mammoth number of heterogeneous devices that are expected to be in IOT network, the architecture is one of the primary issues that must support and manage such type of a network. Also appropriate privacy and security measures need to be in place to effectively secure the communications and storage of huge amounts of data generated. In order to create a system that is effective in its implementation, multiple factors including availability, reliability, management, interoperability, and robustness must be ensured. All of these factors pose specific challenges in the development of an IoT system [4].

Manuscript received April 11, 2020; revised June 29, 2020.

Bilal Ahmad Pandow is with Department of Commerce, University of Kashmir, Hazratbal, Srinagar, J&K (e-mail: ibilalhussain@gmail.com).

Alwi M Bamhdi is with the Computing College in AlQufudah, Umm Al-Qura University, Saudi Arabia (e-mail: saambamhdi@uqu.edu.sa).

Faheem Masoodi (Corresponding author) is with Department of Computer Science, University of Kashmir, India (e-mail: masoodifahim@uok.edu.in).

DOI: 10.7763/IJCTE.2020.V12.1276

II. Existing Literature

There is a plethora of studies available on the subject of Internet of Things and the researchers globally have studied many facets of the IoT. The researchers have shown how social-media platforms have transformed interaction of people and sharing their experiences. While the payment-platforms have disrupted the traditional financial-industry. Even the peer-to-peer digital-platforms created the newly coined term ‘shared economy [5].

Given the scenario, the researchers in [6] have presented a cloud-centric visualization for global implementation of IoT. The important permitting know-hows and application areas that will probably drive IoT exploration in the future have been discussed. The cloud operation consuming Aneka, is grounded on collaboration of public and private clouds. They conclude by mentioning the need for conjunction of wireless sensor network, internet and distributed-computing focused at high-tech exploration society.

While, others [7] have conducted survey and found that IoT can enable global connectivity, also can bring in efficiency in sectors like healthcare visa-via logistics, therapy, diagnosis, recovery, management, medication, and finance. There are books [8] written on the subject that talks about how the electronic-world will transform billions of people into organic-nodes in an array of podiums were we can aggressively harvest and devour produces and connections. The people will be capable to create and share produces, thoughts and community actions on the internet where things will be connected through electronic devices.

Also, there is a study [9] which suggest that IoT-devices and gears with implanted antennas and actuators produce huge volumes of data and then passes it on to business-intelligence and analytics apparatuses for human being to make conclusions. These data are used to determine and decide commercial concerns such as variations in client conducts and marketplace circumstances to upsurge client consummation, and to provide value-added-services to consumers. Similar concerns were raised by Glova [10], where he mentioned that internet-based-technologies has shortened the life-cycles of services and product, hence demanding quicker altering commercial models.

Besides, there are studies by Zhibo et al [11] that suggest two-interfaces to connect the commercial implementation and technology-exploration which will correspond to information conversation amongst the two sides. The significance of this framework is the information interchange by recitation of essentialities from commercial point of view and information for technology use. This information exchange is knowledge blend amongst several themes oscillating from IT, management, engineering, finance etc. Once the data necessities and evidence transfer equals well, the commercial profits can be brought to customers with adequate gratification.

Also, the researcher in [12] has shown that the food-traceability-system has been hosted in many states to decrease the doubts making in the nutrition buying procedure by providing data about the whole food-process, from farm-to-table, in terms of safety and quality.

In addition, the studies carried out in [13] found that the management-accountants cherry-picked the IoT as their object due to the influence that its connectivity has on numbers-collection, exploration, and the decisions-making that follows.

Worth mentioning here that the IoT is expected to renovate lifetime-costs. It will move repairs cost from a time-based action to a need-based action and will track the routine of an instrument in real-time and will exhibit instantaneously when the running-costs will move out of normal-range. Also, it is projected that by 2020 there would be 30 billion product of IoT in-use [14].

Based on the above cited literature review, there is a clear gap in term of financial perspective of IoT industry especially the corporate finance of the firms involved in the IoT industry at various levels.

III. Growth and Development

The IoT functions on three-levels: hardware, structure and application. There have been estimates presented in [15] that suggest that a modest, minor IoT mission cannot cost less than USD fifty thousand. Notwithstanding the challenges like price, privacy and security, the analysts Kobie [16] believe that IoT industry is expected to grow to 4.9 billion connected things in 2015, and is expected to reach 25 billion by 2020.

There is a report [17] that talks about how historical cost of sensor has gone down from as much as USD 15 to as low as 10 cents thereby meaning that practically everything from coffee-cups to aircraft can be fitted with a connectivity-sensor.

A. Geographic Concentration

We analyzed the geographical concentration of the IoT companies as could be seen in cf. Fig. 3 and found that out of total 800 companies surveyed in this paper, more than half which is 445 companies are based in US followed by UK, Canada, France and Germany. In order to achieve inclusive growth spread over globally, the companies should foray other less developing countries. This will not only ensure the wide spread base for IoT companies but will pass on the financial benefits to end-users globally. The geographical distribution of the IoT industry would not only make it more efficient but effective as well in terms of cheap labor and raw material available in the emerging economies. The geographical distribution of the IoT industry would not only make it more efficient but effective as well in terms of cheap labor and raw material available in the emerging economies.

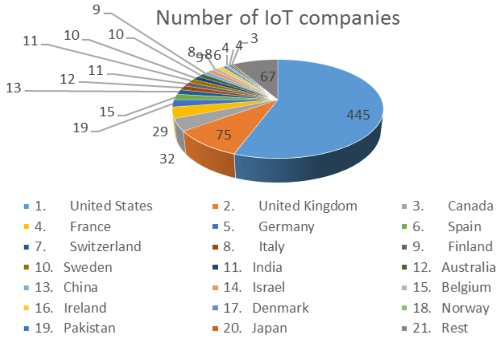

Fig. 3. Global distribution of IoT companies.

B. Product Diversification

Besides, as an be observed in the cf. Fig. 4, In the survey, we also found that most of the IoT companies are concentrating more of these products, having rankings in order of smart watches tops the list, followed by smart bulbs, smart trackers, smart thermostat, smart cameras and many others.

As matter of fact, the companies have to focus also on the product diversification and have to shift their focus from the one product which is the smart watches and takes almost half of the share while other products don't have that much of the share. It has to be proportional to the market demand of the products.

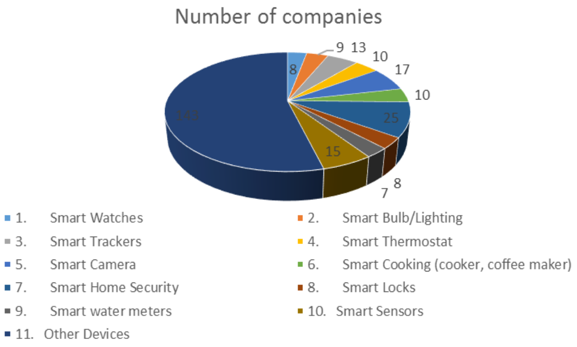

Fig. 4, Device wise distribution of IoT companies.

C. Financial Aspects

In order to ascertain the corporate financial wellbeing of the IoT companies we studied the mean returns of the select five companies for the period of past five years starting from 2013 till 2018. These companies include Spirent Communications, Infenion Technologies, Nuance Communications Inc., Silicon Laboratories Inc., and B-Scada Inc.

As can been observed in the cf. Fig. 5 the financial returns were plotted since May, 2013 till April, 2018. Also, it can be seen that the range of the returns of these companies were between 1.2 to 1.3, however, the industry witnessed a sharp dip in the initial quarter of the 2016 and by the middle of 2017 the returns recovered in the range of 1.2 to 1.25. Also, based on the log trend it was ascertained the trend logarithmic equation: Y = -0.173ln(x) + 3.0797.

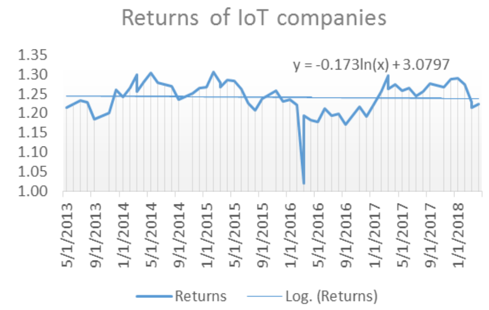

Fig. 5. Financial returns of the select IoT companies.

Though the industry has not witnessed high volatility in terms of the financial returns and is considered as one of the measures by the potential investors before inventing in the existing companies or in the start-ups in the same industry.

D. Future Projections

While, the need of the hour is to bring smart asset monitoring system. As also pointed out by the study in [18], implementing IoT would mean bringing in smart-asset-monitoring system which is forecasted to bring higher return on asset and better assistances to firm's revenue. Recognizing the value from such a solution is an extremely dedicated resourcefulness and will depend on 3 things predominantly: involvement of the entire-organization, capability to generated data and ability to renovate the process in the companies.

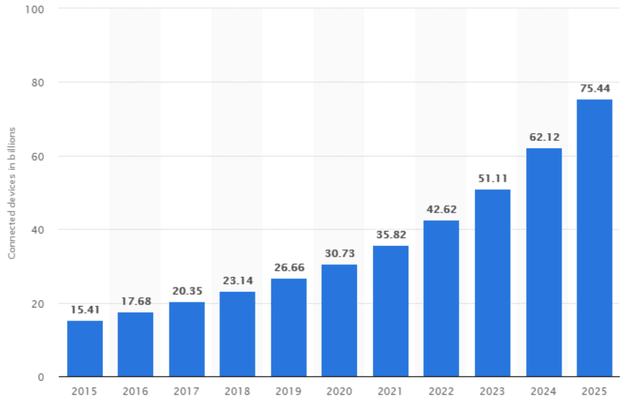

Fig. 6. IoT connected devices installed base worldwide from 2015 to 2025.

Besides, the IoT connected devices installed base globally since 2015 to 2025 (in billions) can been seen from the cf. Fig. 6. By 2020, the installed base of IoT devices is expected to grow to 31 billion globally. An enormous USD 19 trillion is projected as cost-savings and net-profits from this investment [19]. Also, major acquisitions are taking place in this area like Google acquired Nest Labs for USD 3.2 billion and Samsung, bought SmartThings for USD 200 million.

IV. Security Concerns

The digital revolution has played a vital role in finance industry. Due to the availability of verifiable real time data, the process of financial decision-making has become swift and easier. With the establishment of IoT, financial industry can obtain and analyze vital information from heterogeneous sources to propel profit surge. Though Internet of things seems to be an ideal growing platform for financial industries but the evolution is inhibited by the critical issues like security, trust, privacy, integrity and availability. One of the major issues currently faced by IOT is the concern for privacy and security of involved stakeholders. While as Privacy includes the concealment of personal information as well as the ability to control what happens with this information [20], [21], IoT security is concerned with safeguarding "things" in the Internet of things. IoT systems are prone to security attacks for a variety of reasons including the wireless communication between devices, physical access to objects, constrained capacity of smart devices and openness of the system [22]. Broken devices or permanent failures of such devices provide vulnerabilities and can therefore be exploited by potential attackers. A typical example of such devices can be RFID tags.

What makes privacy an intrinsic IoT requirement lies in the anticipated IoT application domains and in the technologies used. IoT adoption is harnessed due to lack of adequate measures for ensuring privacy of information in variant IoT application fields like patient’s remote monitoring, energy consumption control, traffic control, smart parking system, inventory management, and production chain etc. [23]. Additionally the adoption of wireless communication medium for data exchange can lead to potential risk of privacy violation as exchanges over such medium can expose the underlying system to multiple attacks. Under these circumstances, security and privacy represents a real research challenge that may restrict IoT development.

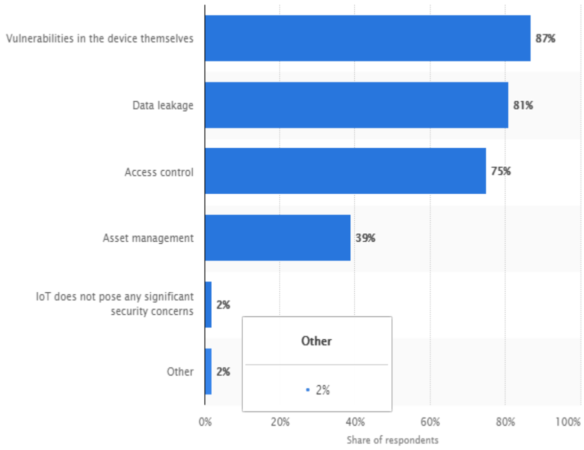

Fig. 7. IoT security issues experienced by users; Source: Statista.

According to the report published by director of finance in June 2017 [24] IoT attacks have been carried out on half of US financial firms resulting in an approximate breach cost of $20 million for big companies. A significant number of users are wary of security issues like data leakage, IoT device being taken over by hackers, missing security standards IoT vulnerability scans, enterprise interoperability, asset management etc.

The need of the hour is to develop a consensus about how IoT security can be implemented. A multi-facet strategy that would address the potential threats including intrusion from external sources, authentication, access control, authorization, recovery from crashes, software security and interoperability. The idea is to create a robust platform with transparent and secure framework to mitigate these potential threats.

V. Conclusion

The IoT revolution is having the capacities to make today’s industries extra-effective, more-sustainable and cost-effective. In order to take full advantage of the IoT technology, the cost befit analysis of its implementation in any sector will assist the decision makers to opt for the IoT. As also pointed out by [17] the champions in the IoT are the firms that comprehend how to intertwine IoT-technology into the products to standout of the traditional-competitors. While as those who can’t are expected to brawl to stay alive. And it is in the interest of the companies to invest in IoT and make it their top priority as IoT is expected to evolve at an unbelievable speed in the next-decade.

While, based on the research survey and finding of this paper out of the 800 firms, 445 are based in US, followed by United Kingdom, Canada, and Germany which needs to be a matter of concern for the overall development and growth of the IoT industry. The geographical distribution of the IoT industry would not only make it more efficient but effective as well in terms of cheap labor and raw material available in the emerging economies. Also, the companies have to focus on the product diversification and have to shift their focus from the one product which is the smart watches to others as well.

Besides, it was observed that the financial returns of select IoT companies for past five years have witnessed a decent growth however; the industry witnessed a sharp dip in the year 2016. Though the financial returns over the years have recovered however, these dips makes them risker and this is a matter of grave concern for the investors who could potentially fund the new and existing IoT ventures in the future. While, there are number of mergers and acquisitions that took place in the IoT-industry coupled with the demand of IoT products in the market, the industry is expected to cross and achieve a growth of USD 75.44 billion mark by the year 2025.

The whole idea of implementing IoT finance cannot be successfully executed unless the security and privacy concerns become part of the roadmap. Absence of robust communication protocols, uniform security standards and strong data regulations act as serious impediment to the IoT security.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Since we all are from different fields, each one of us has contributed to this paper accordingly. Faheem Masoodi has contributed in term of IoT security, while Bilal Ahmad Pandow contributed to the financial dimension of this paper and Alwi M Bamhdi in growth and development of the IoT globally. All authors have approved the final version.

References

[1] R. Payne and B. MacDonald, “Ambient technology — Now you see it, now you don't,” *BT Technology Journal*, vol. 22, no. 3, pp. 119-129, 2004.

[2] Y. Lu, S. Papagiannidis, and E. Alamanos, “Internet of Things: A systematic review of the business literature from the user and organisational perspectives,” *Technological Forecasting and Social Change*, 2018.

[3] S. Sarma, “Towards the five-cent tag,” *MIT Auto-ID Center White Paper*, 2001.

[4] H. Sarra, Z. Aliouat, and S. Harous, “Challenges and research directions for Internet of Things,” *Telecommunication Systems*, pp. 1-19, 2017.

[5] M. Reuver, C. Sørensen, and R. Basole, “The digital platform: A research agenda,” *Journal of Information Technology*, 2018.

[6] J. B. Gubbi, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[7] H. Xu, “Internet of things in industries: A survey,” *IEEE Transactions on industrial informatics*, vol. 10, vol. 4, pp. 2233-2243, 2014.

[8] J. Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, St. Martin's Press, 2014.

[9] I. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” *Business Horizons*, pp. 431-440, 2015.

[10] J. S. Glova, “Business models for the internet of things environment,” *Procedia Economics and Finance*, pp. 1122-1129, 2014.

[11] Z. Pang, “Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion,” *Information Systems Frontiers*, pp. 289–319, 2015.

[12] Y. C. Choe, “Effect of the food traceability system for building trust: Price premium and buying behavior,” *Information Systems Frontiers*, pp. 167-179, 2009.

[13] C. Mishler, “The future of the internet of things,” *Strategic Finance*, vol. 62, 2015.

[14] T. Davis, *The Macroeconomic Implications of the Internet of Things*, Solair Corporate, 2012.

[15] P. Piletic. (2018). Datafloq. [Online]. Available: https://datafloq.com/read/internet-of-things-cost-build-iot-solutions/4448

[16] N. Kobie. (2015). The internet of things: convenience at a price. [Online]. Available: https://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security

[17] Z. Kerravala, “It’s time for businesses to embrace the Internet of Things,” *A ZK Research Whitepaper*, 2014.

[18] R. Rajan, *Increasing Your ROA (Return on Assets) with IoT (Internet of Things)*, United States: Rapid Value, 2017.

[19] Statista. (2018). The statistics portal. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[20] J. Stankovic, “Research directions for the Internet of Things,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[21] F. Masoodi, S. Alam, and S. T. Siddiqui, “Security and privacy threats, attacks and countermeasures in Internet of Things,” *Int. Journal of Network Security and Its Applications*, vol. 11, pp. 67–77, 2019.

[22] S. Sicari *et al.*, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146-164, 2015.

[23] M. Smith. (2017). Director of finance. [Online]. Available: http://dofonline.co.uk/2017/06/05/cyber-security-half-firms-iot-breached/

[24] H. Kopetz, “Internet of things,” in *Real-Time Systems*, Boston, MA.: Springer, 2011, pp. 307-323.

Bilal Ahmad Pandow was a researcher at the University of Kashmir, until recently he became a senior lecturer in the Department of Management Studies, Middle East College, Muscat. He previously served in the University of Kashmir for a period of over six years. He has MPhil (finance), masters in finance and control, and PGDCA to his credit. He is also a certified microfinance trainer with the Asian Development Bank Institute and the World Bank—Tokyo Development Learning Center. He has published 15 research papers in leading journals.

Alwi M Bamhdi is an assistant professor in the Department of Computer Sciences, Umm Al-Qura University, Saudi Arabia. He received his MSc and Ph.D. in computer science in 2014 from Heriot-Watt University, UK. His research interests include mobile ad hoc networks, wireless sensor networks, information security, internet of things, cyber security, computer vision and simulation and performance evaluation.

Faheem Syeed Masoodi is currently working as an assistant professor in the Department of Computer Science, University of Kashmir. Earlier, he served College of Computer Science, University of Jizan, Saudi Arabia as an assistant professor. Prior to that, he performed his duties as a research scientist at NMEICT-Edrp project sponsored by Ministry of HRD, Govt. of India in 2015. He was awarded PhD in the domain of network security & cryptography by the Department of Computer Science, Aligarh Muslim University India in year 2014 and did his masters in computer sciences from University of Kashmir.

His basic research interests include cryptography & network security; and internet of things (IOT). He is a professional member of many cryptology associations and has published multiple research papers in reputed journals and conferences. He has been awarded fellowship for summer training “Conference effective moduli spaces and application to cryptography” organized by Centre Henri Lebesgue, Rennes, France in 2014 and was also awarded fellowship for summer school “SP-Ascrypto-2011 Advance School of Cryptography” at University of Campinas, Sao Paulo, Brazil in 2011. He was also awarded Maulana Azad National Fellowship for his doctorate programme by UGC New Delhi. His teaching interests include cryptography and network security, theory of computation and design and analysis of algorithms. Dr. Masoodi is also course coordinator of MOOC course “Design and Analysis of Algorithms” https://swayam.gov.in/nd2_cec20_cs03/preview.