IoT Challenges: Standardization

Danish Zaheer Malik
Electronics Engineering
Hochschule Hamm Lippstadt
Lippstadt, Germany
Danish-zaheer.malik@stud.hshl.de

I. Abstract

Over the previous few years, the Internet of Things (IoT) has grown in popularity and usage by leaps and bounds. The relevance of IoT in the lives of industries, technologists, and home users is well understood. Essentially, the Internet of Things (IoT) has brought in a massive industrial revolution and has aided in the automation of numerous activities in businesses and homes. The rapid rise of IoT, on the other hand, is a significant source of concern not only are security, authentication, and privacy issues plaguing IoT, It also doesn't work as effectively as it should with access control issues. Industry 4.0 refers to the fourth industrial revolution because of inadequate governance norms and regulations, device security and IoT network security have deteriorated over time, as well as a wide range of privacy problems. This study explores the Internet of Things market and highlights the vital need for standardization, the advantages of governance, and the issues that the IoT area suffers as there is not enough regulation. Internet of things security framework is also introduced in this study for organizations in order to deal with the existing absence of rules in the Internet of things market. Implementing the strategy outlined in the recommended structure will aid organizations in achieving privacy, security, scalability and long-term viability, in their IoT networks.

II. Introduction

Little more than 30 years ago, Windows 3.0 is the 3rd major edition of Microsoft Windows, released in 1990 which was heralded as a game-changing triumph. Its multitasking features figure 1 [16] and user-friendly graphical interface impressed customers. Today, Internet of Things (IoT) gadgets surround us and systems that use very slight memory yet can perform considerably more complex computations than Windows 3 could in the 1990s [7].

[1] The Internet of Things has generated a huge network of connected gadgets that are continually communicating with thousands of other objects connected to the internet. The massive expansion of the Internet of things business is having enormously good consequences on humans, and the Internet of things has brought man and technology closer together. One of the benefits of this technology in the business sector is its ability to support Industry 4.0, technology, effective data collection, and service costs . Furthermore, The Internet of Things is being utilized to intelligently monitor, identify, analyze the environment, and manage critical infrastructure. However, the absence of regulation in the industry, which is still considered to be in its infancy, has hampered IoT development. The International Organization for Standardization (ISO) has conducted multiple studies, the most recent of which was completed within the previous decade, to settle on the financial benefits of standardization for rising technology companies .

According to some approximation, there are trillions of Internet-linked things. As IoT devices acquire, transmit, store, and analyze data in an inconspicuous manner, it is becoming increasingly vital for them to function securely . However, the market suffers from unregulated IoT proliferation because of a lack of defending norms, regulation, and universal standards . Many of the technology's makers, developers, and facilitators work without control or respect for security, resulting in a lack of security across the IoT network as a whole. Whilst certain recent advancements in the field of standardization, like as the United Kingdom Government's Secure by Design Initiative, have addressed industry apprehensions, they do not fully address them. Furthermore, present standards and projects only cover a tiny percentage of IoT components and services.[12,7]

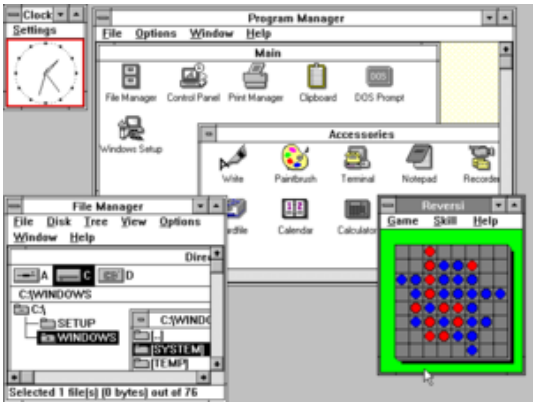

Fig. 1. Snap of Windows 3 multitasking features

III. STANDARDIZATION IN SCIENCE

While discussing standards, it's crucial to first understand why they're being implemented in the first place. A standard's principal goal is to systematize the application of instructions. A standard attempts to codify an agreement on how to carry out an operation, create a product, measure an item, or

offer a service. Standards can assist organizations in applying instructions and commands consistently across the board in this way. Moreover, the same standards can be used to measure conformity with the original instructions at a later time.
There are now hundreds of regulations covering anything from the safety of toys to the safety of nuclear power plants. Widespread scientific research, collaboration linking academics, industry, and legislative organizations are all used to create effective standards. Organizations accept standards once they have been finalized. In the design of successful standards, sector specialists' involvement is crucial, since it indicates both a grasp of the topic an awareness of the expectations of their manufacturing industry [15].
Standardization not only improves the quality of products and service but it also assists the growth of scientific knowledge. The case of 'Drosophila,' perhaps is the most well-known example of such development. The standardized fruit fly which has resulted in substantial genetic advancements. Drosophila experiments in 1916 were the first to show that chromosomes have genes on them. As a result, in the year 2000, Drosophila was 1st creature to get its full genomic sequencing done.
When IBM created and standardized private networking systems like TCP/IP in the late 1980s, the first phase of standards in the field of information technology has been established. In the 1980s, when the Internet started to develop as a foundation for low-price communication and information sharing IEEE 802.3 was developed as a standard for 10Mb/s Ethernet. Standards in the communication sector focused on system optimization to enable new services like data transfer, email and telephony. While, in the information technology industry, the next generation of standards aimed at improving quality of service (QoS) in order to fulfill end-user demand for multimedia services [5].

IV. International Standardization Organizations

Because of the enormous complexity of Industrie 4.0, there will not be a single Industrie 4.0 standard in the medium future. Instead, over the next several years, a plethora of standards, some very specialised and others more generic in character, will develop to provide interoperability in and between a wide range of systems and at various levels [4].
For the Internet of Things and Industry 4.0, there are several Standardization projects now underway. The EU's Alliance for Internet of Things Innovation created Figure 2 [4] (AIOTI). It lists some of the currently active Standards Developing Organizations (SDOs). In this vast subject, more than a hundred Standardization Organizations of varied prominence are presently operating. Because the environment is always changing and key Standardization Organizations are developing concurrently in specific sectors, it's difficult to say which of them are relevant to Industry 4.0. As a result, it's critical to keep a close eye on individual regions, technology themes, and sub-domains, as well as to identify and update the necessary Standardization Organizations on a regular basis [4].

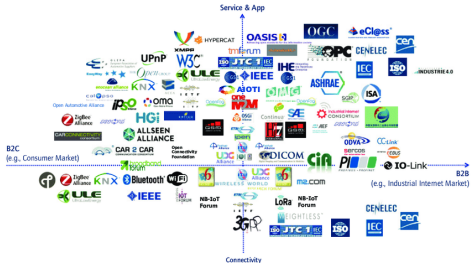

Fig. 2. Organizations that work to standardize the Internet of Things

V. Advantages of Standardization

Standardization is critical not only for IoT but for every new and developing technology, as it saves the time and effort required to collect fundamental data and determine the area for testing. Standardization in IoT aids in lowering the total cost of data generation, safeguarding the system by discovering security flaws, and closing gaps across protocols. Standardization reduces the entire time frame and cost of manufacturing innovative products, which helps support the industry [16] .
IoT standards ensure that solutions and products are appropriate for their intended use. Specifically, communication technology is rigorous in order to give high quality-of-service, toughness against industry-grade, and interference to enable the secure transmission of huge IoT Sensors at the edge .
To facilitate multi-vendor solutions and the integration of heterogeneous devices, standardized communication orders may be performed on various commodity off-the-shelf hardware such as gateways and chipsets. Aside from long-term interoperability, this helps end-users avoid the business risks of vendor lock-in, in which a single provider holds ultimate power over functionality design and planned product/technology upgrading.
Industrial customers with large operations seek to adopt IoT connections that can be delivered across several foreign locations. Standardized extracts work worldwide and assist to reduce wiring complexity, which is critical for protecting long-term investment [3].
Customers and users often see producers who comply with industry standards as more reliable and trustworthy. Customers see conformity as proof that things have been manufactured and tested using tried and true procedures. Standards compliance also assures that the completed product is of good quality and will work as intended. This guarantee effectively gives the client confidence that the item is in good and safe hands, dependable, and performs as intended. Some other advantage of standard compliance that leads to approval is that it improves the company's and its products reputation. This image may assist firms in thriving, prospering, and achieving their financial goals.
Standards, on the other hand, not only contribute in the development of safety, quality, and environmentally friendly policies, however they also aid in the improvement of organizational and economic performance. The long- term

viability of the Internet of Things is strongly reliant on efficient standards; this must include all areas of Internet of things technology , development and lifetime management, from product design and production to repairs, warranties and software upgrades, dismantling, care, and removal. Using a universal standardized interface for application development environments, Standardization will also facilitate collaboration on security and other fronts of development. As a result, standardization can provide much-needed control and maturity, which is critical for overcoming the existing IoT security and dependability challenges [7].

VI. Problems driving the standardization debate in the IoT industry

he Internet of Things is recognized to have dependability and security difficulties. The IoT industry as a whole is facing significant hurdles, which are becoming more severe as usage grows and advances. Vulnerabilities in IoT devices give hackers easy access, leading to more hostile attacks, data theft, data destruction, and hardware damage. Moreover, ”pwned” devices allow for huge simultaneous attacks on Information Technology infrastructure, with victims bearing the brunt of the repercussions beyond geographic boundaries. The following are some of the significant concerns affecting IoT [8].

A. Security

Wireless communications, sensors, Radio-Frequency Identification (RFID), and machine to machine connection all are part of the Internet of Things (M2M) as shown in figure 3 [11] the M2M applications. The IoT market, on the other hand, is still unregulated, which has resulted in broader safety and confidentiality problems. The widespread usage of unsecured Internet of things devices in practically all fields, including military and health Care , as well as their rising popularity among consumers, has resulted in the creation of a new attack vector. It is scary how easily IoT devices can be hacked, and data packets can be intercepted.

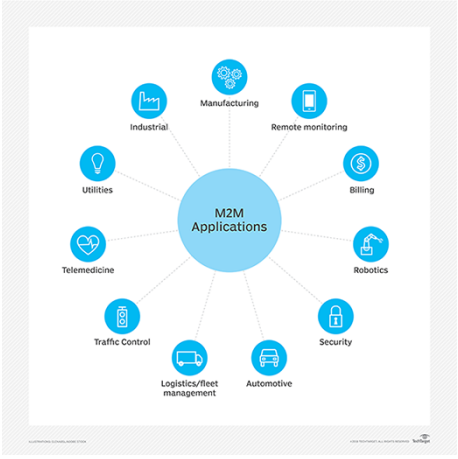

Fig. 3. M2M Applications

The sorts of threats that target IoT are depicted in Figure 4 [7]. Such attacks can occur at any level of the IoT protocol stack and are heterogeneous in nature. Because of their proliferation in important infrastructure, including the power grid, transportation, railway, smart cities and healthcare sector, In recent years, the danger of economic, and bodily damage from compromised Internet of things devices has skyrocketed. Despite the fact that the company was concerned about safety issues, prominent internet attacks, such as the one on DYN's network , which leveraged One Hundred Thousand hacked IoT devices, have pushed the issue to the fore. Stuxnet and other similar assaults had an unintended consequence: they raised public awareness about the requirement for legislation, effective security proce- dures, and tighter restrictions over authentication of Internet devices [7].

Fig. 4. A overview of IoT types of attacks

B. Interoperability

Interoperability is significantly hampered by the growing number of components, languages, data layers, and supporting soft and hard wares used in the creation of an IoT system. The services listed above should, in an ideal world, function well together to improve compatibility and information flow. Several attempts have been made in the industry, like Apple's HomeKit, to connect several IoT devices from different producers into a unified user interface. Similarly, Samsung's Smart things Hub has features that are almost identical to Apple's HomeKit, however both systems are limited in terms of the amount of devices that may be utilized with them. As a result, interoperability standards are desperately needed.
Due to heterogeneity, interoperability concerns in IoT may be seen from several viewpoints. Even in the physical world, there are many different sorts of heterogeneities. For example, persons who speak different languages can converse with one other using a translation tool or a common language. Similarly, the many pieces that comprise IoT (electronics, connectivity,

services, applications, and so on) must smoothly collaborate and interact with one another in order to fulfill the full potential of the IoT ecosystem. As shown in Fig. 5 [14], IoT interoperability may be examined from several viewpoints, including devices interoperability, syntactic , semantic interoperability, and platform interoperability [14].

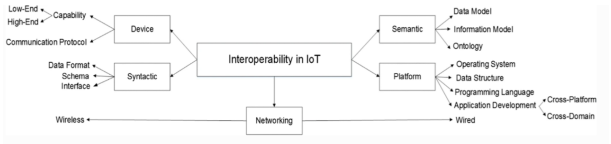

Fig. 5. IoT taxonomy

VII. Analysis of the standardization outlook in the IOT industry

Nowadays we are entirely surrounded by IoT gadgets. It's unusual to be seeing lights turn on when they sense a person's existence, or heat, ventilating, and central air systems turn on when the temperature falls below or surpasses predetermined thresholds. voice-activated gadgets with always-on virtual assistants are getting more popular. Precision voice analysis is included in such gadgets, allowing the digital assistant to assist the user with everyday tasks.

Our cities, too, are becoming smarter. These devices, for example, are used to regulate parking, assess traffic, track residents' activities, allowing them to examine shifting metropolitan trends. Smart sensors are being utilized in commercial businesses to monitor and maintain facility environments, such as the temperature within medical storerooms facilities or medical transport trucks, and the tracking of delicate or costly items. In the case of an incident or accident, automobiles are also equipped with IoT devices that may convey real-time trouble alerts to rescuers and responders.

IoT has had a significant impact on modern economies and continues to present many prospects for citizens and the digital market. On the other hand, the combustible growth of the Internet of things is a big source of concern. The industry's standardization has fallen short of the retail, commercial and private sectors' extensive and rapid adoption of IOT . The IOT industry has become a popular target due to weak validation, encryption, and attack anticipation systems, Furthermore, these flaws have resulted in consequences as an example of decreased user confidentiality. Because of the huge percentage of poorly secured Internet of things devices, big-scale cyber assaults, including state-sponsored attacks, are also a risk.

The above- mentioned dangers can be mitigated by enacting rules and laws geared specifically at the IoT business. However, even when the regulations are implemented, it is estimated that the chance of total compliance in the manufacturing industry would be low for a brief period. There are a variety of causes for this delay in compliance. For starters, there is now no direct motivation for manufacturers to make such adjustments because manufacturers are rarely the targets of cyber-attacks and hence have little firsthand knowledge of the financial consequences of cyber-attacks. Second, the cost of compliance, higher resource requirements, and a skills scarcity in the software business might all function as big deterrents for manufacturers. Governments are said to need to create compliance incentives in order to induce compliance. Standard compliance would boost consumer confidence as well as the security of Internet of things systems against cyber assaults. Government subsidies might be utilized to encourage people to follow the 'No Trust' paradigm and the 'Safe by Default' strategy [2 ,7].

A. Intervention by the Industry

The need for regulatory oversight in the IoT sector necessitates immediate response. Standardization in the IoT business is a complex and difficult issue from the standpoint of governance. The development of the most stringent set of criteria for a wide range of sensors, microcontrollers, connections, actuators, and programming platforms from around the world is a complex effort that necessitates collaboration among numerous international organizations. Nonetheless, the sector has recently made certain steps at a national level:

The Industrial Internet Consortium (IIC) was founded in the year 2014 with the goal of accelerating the growth of connected devices. The organization hopes to build a cooperation of global corporations, governments, and universities to focus on the development of real-world test beds. In addition, the business has keenly advocated for the need for values in the internet of things manufacturing sector [6].

Internet Task Force (IETF) is an organization dedicated to developing recommendations for Internet linked devices. Established in 1986, the Internet Engineering Task Force (IETF) has recently shifted its focus to the Internet of Things, encouraging developers and manufacturers to embrace its rules on a voluntary basis. Their current work involves the expansion of a steering method draft for Routing Across Light Power and Lossless Networks and the definition of a collection of procedures to help IPv6 over low powered Wireless Personal Area Network (6LoWPAN) [9].

IoT Security Foundation (IoTSF) Since the year 2015, a organization that has been assisting the IoT business. IOTSF has acknowledged the problems in the sector and is attempting to link the gap by working together with rms that deal with IoT to develop rudimentary training, courses and privately established IoT security guidelines. The IoT Security Foundation also provides an IoT framework in the form of a check-list in addition to the aforementioned. IoT manufacturers should be encouraged to self-certify and deploy their IoT Security Foundation framework [10].

Furthermore, the code of practice lacks substance and depth, as well as technological industry requirements. The document contains an overview of IoT problems as well as a 13-point generic industry proposal. For instance, There are 114 controls in the ISO 27001 standard, which focuses on IT infrastructure security. They are grouped into 14 clauses and 35 control categories. The discipline of a privacy-oriented and safe IoT economy is missing within the maze of advanced ter-

minologies, technologies, and problems surrounding the IoT. For the Internet of things industry to grow strong, efficient, and consistent for customers, regulations are essential. For far too long, the industry has been left to govern itself on its own, and the data shows that this method has failed.

Recent Cambridge Analytica concerns include its role in illegal Facebook data gathering, election interference in the US, Kenya Nigeria and Manipulation of voters in the Brexit vote. Each one of these crises has shown What can be done when personal information falls into the hands of the wrong people [7]. The flood of investigations and criticism that has landed on Facebook in the aftermath of disclosures of large amounts of data misuse, as well as Facebook's first weak response, is to be commended, but the risk of data exploitation posed by unmanaged IoT gadgets continues to escalate. It's critical that customers don't suffer the repercussions of subpar devices, which are susceptible due to IoT manufacturers' poor design, weak authentication measures and inadequate encryption. As a result, the activities detailed in this section start to show some results. However, it is evident that the self-regulation criteria of the government do not completely address valid security issues but also do not depict the future visualization of safe IoT devices [13 ,7].

VIII. CONCLUSION

The IoT business has seen a tremendous increase in income as a result of the popularity of devices offered for smart homes, industrial, and medical monitoring. The best-selling items in 2017 were security cameras, locks, thermostats, lighting, and smart assistants. Despite its success, the IoT business today is confronted with two major difficulties that must be solved as quickly as feasible. The first issue is a lack of security in IoT devices, which has resulted in the introduction of new attack vectors and millions of cyber security flaws. Attackers are aggressively exploiting these inherent IoT device flaws. Second, there are no industry wide standards for IoT.

loT sector now a days faces a significant requirement to adopt and implement a unified framework that has been developed, assessed, and verified by professionals. The industry's acceptance of the proposed Internet of things Security Framework would not only help with knowledge, it will not only provide insight into potential design for less experienced manufacturers, but it will also provide them with an awareness of the procedures required to achieve an acceptable level of security in Internet of things items. The security of loT devices in the industry will improve as a result of growing adoption and compliance with this framework, and by this customer trust will rise.

REFERENCES

[1] Ali Benzerbadj, Bouabdellah Kechar, Ahcne Bounceur, and Mohammad Hammoudeh. 2018. Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links. J. Netw. Comput. Appl. 112, C (June 2018), 41–52. DOI:https://doi.org/10.1016/j.jnca.2018.03.027

[2] S. Walker-Roberts, M. Hammoudeh and A. Dehghantanha, "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure," in IEEE Access, vol. 6, pp. 25167-25177, 2018, doi: 10.1109/ACCESS.2018.2817560.

[3] https://tudip.com/blog-post/why-iot-standardization-is-important/.

[4] Kagermann, Henning Anderl, Reiner Gausemeier, Jürgen Schuh, Günther Wahlster, Wolfgang Winter, Johannes. (2016). Industrie 4.0 in a Global Context: Strategies for Cooperating with International Partners (acatech STUDY).

[5] David D. Clark * Massachusetts Institute of TechnologyLaboratory for Computer ScienceCambridge, MA. 02139 (Originally published in Proc. SIGCOMM '88, Computer Communication Review Vol. 18, No. 4,August 1988, pp. 106–114

[6] "Industrial Internet Consortium". www.iiconsortium.org. Retrieved 2021-05-08

[7] Saleem, Jibran Hammoudeh, Mohammad Raza, Umar Adebisi, Bamidele Ande, Ruth. (2018). IoT standardisation: challenges, perspectives and solution. 1-9. 10.1145/3231053.3231103.

[8] Ghafir, Ibrahim Saleem, Jibran Hammoudeh, Mohammad Faour, Hanan Prenosil, Vaclav Jaf, Sardar Jabbar, Sohail Baker, Thar. (2018). Security Threats to Critical Infrastructure: The Human Factor. The Journal of Supercomputing. 74.10.1007/s11227-018-2337-2.

[9] IETF. 2018. (2018). https://www.ietf.org/

[10] IOFSF. 2018. (2018). https://www.iotsecurityfoundation.org/

[11] https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M

[12] Meddeb, Aref. (2016). Internet of things standards: who stands out from the crowd?. IEEE Communications Magazine. 10.1109/MCOM.2016.7514162.

[13] Jason Parham. 2018. FACEBOOK AND THE PRICE OF TECH UTOPIA. (Mar 2018).

[14] https://link.springer.com/article/10.1007/s11036-018-1089-9

[15] https://en.wikipedia.org/wiki/Windows3.0

[16] https://intellipaat.com/community/63491/why-is-standardization-important-for-iot

IX. Declaration

I , Danish Zaheer Malik, student of Bachelors of Electronics Engineering at Hochschule Hamm-Lippstadt, hereby, declare that the work presented in this research Report has been carried out by me with all proper references and I also announce that I did not send this report to any other institution for the grant of any degree of qualification.