Software Evolution Challenges in IoT

Gilles Schneider
40171011

Saswati Chowdhury
40184906

Sepehr Seifour
40197899

Vaibhav Sharma
40197697

Abstract*— The Internet of Things (IoT) is a concept that refers to the billions of physical devices which are connected to the internet that gather and share information. The aim of evolving this concept is to develop a real time platform to communicate with the world more efficiently, smartly and quickly without depending on a system by human intervention. As the number of connected devices continues to grow, this rapidly changing environment raises challenges and threatens the capability of a software system to evolve. Therefore, it is crucial to establish these challenges to prevent IoT devices software from declining. In this paper, we analyzed sone research papers that tackle one or more recent challenges and made a comparison to anticipate future directions.

Keywords*— Internet of Things; Background; Software evolution; Future directions.

I. INTRODUCTION

The number of interrelated devices communicating through the Internet is exponentially increasing. These devices are part of the so-called Internet of Things (IoT). From smart cities to healthcare, IoT devices are everywhere. One can think of the Meda Cube's medication dispenser that gives patient medication at the right time along with the instructions on how to take them. Consequently, IoT is subject to cultural shifts. To name a few, they include the reduction of human-machine interaction, industrial automation, and Health 2.0. Also, the emergence of Artificial Intelligence leads IoT devices to simulate smart behavior and support decision making with little human intervention. Moreover, IoT devices are subject to technological breakthroughs and must use new technologies to stay relevant to the market (e.g., cloud computing). Therefore, IoT is a dynamic field where new challenges come to life and software is not spared. For instance, there are emerging concerns about security and users' information privacy at software level. IOT has a brass majority of its application in rugged computers like PLCs – writing software libraries for which require program comprehension of legacy code along with knowledge of third generation languages like Pascal and C. Any extensions made to the legacy code thereby contributes to software complexity and aging. The paper tends to identify and review some of the modern software evolution challenges in IoT. The remainder of the paper is organized as follows, Section 2 will be introducing relevant background information, Section 3 will be reviewing relevant papers about software evolution challenges in IoT, and Section 4 will be discussion the future directions of these challenges.

II. BACKGROUND

This section introducing relevant concepts that will be used throughout the paper.

A. Internet of Things

"The IoT technology can be simply explained as a connection between humans – computer – things". More precisely, IoT can be seen as a network that connects electrical and electronic sensing equipment that humans manage remotely or use to exchange data (e.g., smartphones). Using the Internet to exchange data, IoT devices use agreed network protocols such as WIFI, 4G, etc. In 1990, John Romkey created the first IoT device: he could turn on and off a toaster over the Internet. The term Internet of Things was brought to light by Kevin Ashton (executive direction of the AutoIDCentre, MIT) in 1999. With the rapid growth of the Internet in the past decades, IoT devices became an important part of today's life.

B. Software evolution

According to Lowell Jay Arthur, software evolution means "continuous change from lesser, simpler or worse state to a higher or better state". The main goal of software evolution is to improve a software system. This can include adding new functionalities, adopting a better design, etc. Evolving a software is a challenging process that is highly dependent on its environment. Requirements evolve due to environmental changes and not being able to meet new requirements leads to a progressive decline in software. These challenges are augmented when we realize that IOT devices are built on platforms which foster software written in multiple generations of languages. Porting extensions to these machines require a T-shaped expertise of several developers which can be better achieved by incremental delivery processes.

III. REVIEWED PAPERS

This section reviews relevant papers that tackle software evolution challenges in IoT.

[1] The IoT Energy Challenge: A Software Perspective

Motivations. Powering IoT devices is challenging because these devices can require more energy than what most powering solutions can deliver. Nowadays, most energy-consumption optimization is hardware-based, and little is done with software. Developers ignore the impact of their coding choices on energy consumption because no feedback, called energy transparency, is provided to them. Powering issues often happen at a late development stage, leading to delivery delays and additional costs.

Methodology. Firstly, the paper defines a set of requirements that modern techniques must meet to allow energy transparency (without using reverse engineering). Secondly, it analyzes the state-of-the-art techniques that allow energy transparency and reveals their advantages and drawbacks regarding the requirements. Lastly, the paper draws the remaining challenges.

Findings. Modern techniques must meet the following requirements to provide energy transparency: define bounds of actual energy consumption, study energy consumption at multiple software levels, use software artefacts as much as possible, be independent of architecture or programming languages, usable in multi-threading system, fast and easy to deploy, and provide feedback.

Two main ideas exist to define energy consumption bounds: measuring and estimating energy consumption. The fist is accurate but not feasible in practice. The second has a satisfying balance between feasibility and accuracy.

To estimate energy consumption at a software level, an energy model is required. Such a model associates each unit (e.g., instruction) of a software level with an estimated energy cost. There is a trade-off between the energy modeling precision loss and the software abstraction level. Indeed, it is difficult to estimate the energy cost of small chunks of code (e.g., for loops).

Profiling-Based and SRA-Based Energy Consumption Estimation are the main modern techniques that tend to provide estimate energy consumption bounds. Profiling-based techniques estimate energy consumption at runtime whereas SRA-based statically define bounds. Among profiling-based techniques, one can find simulations, code instrumentations, and performance counters. SRA-based techniques appear to be more practical than profiling-based techniques.

Although these techniques offer satisfying energy transparency, there are remaining challenges. They often overestimate the tight upper energy consumption bound and do not scale well to multi-threaded architectures. Also, energy models assume to only use constant power source, therefore exclude variations in power supplied to the processor. Furthermore, energy models forget to include other electrical components that consume energy such as peripherals or I/O operations. These components sometimes consume even more than the processor. Lastly, the biggest challenge is developer's perception: optimizing energy consumption is seen as an obstacle to development. Most developers hope that compiler does the optimization for them.

[2] A Road to the Programmable world Software Challenges in the IoTs

Motivations. By emerging IoTs, Hardware and objects are expected to be connected to internet. From air conditioner, bubbles and doorknobs to vacuum cleaner. Most conducted research is currently concerned with machine learning, data visualization and other big data topics. Collecting and joining data represents a specific and behavior depicting the importance of this business. This survey demonstrates a road map of today's cloud data centric IoT system to a world where everyday objects are connected. Today's language programming and programming tools or better to say those pervasive ones are poorly provided with suitable manners to tackle the emergence of programmable things.

The article specifies the technical issues and challenges that require more study and deeper comprehension beyond IoT topics that draw more attention today.

Methodology. Most collected data are from observations from trends in industry and academic papers. Personal experience and observation from mobile applications and their revolution. By collecting these data, this article represents a table demonstrating data viewpoint and programmability viewpoint from 2015 to 2025.

Findings. On this article, scientists predict IOT development altering over the coming years. Now, there is no universal, interactive software development environments exists that allows developers to code IOT application capable of running on all types of devices, let alone organize and manage complicated topologies and installations of such devices. Scarce of such tools can have significant implication IOT market's development. We believe that most web-application and ordinary mobile app is not facilitated well to deal with IoT challenges with aspect to distributed systems, the most outstanding of which is reaching the appropriate balance between application logic and error handling. Other issues in developing IoT software, is that most programming language are common in both mobile-app and IoT development such as Arduino, C#, python, java, etc. Meanwhile, JavaScript and NodeJS are becoming rife central tools for developing IoT whereas they are not considered asynchronous, distributed applications. Furthermore, there are also some additional challenges in IoT development with regards to Software evolution such as security, the dynamic nature of IoT system and so forth and so on.

[3] IoT security evolution: Challenges and Counter Measurement

Motivations. This article furnishes a rigorous review of IOT evolution with regards to security issues. By soaring the connectivity of IOT devices steadily, for instance it was calculated that by the end of 2020, the IOT would reach about 50 billion devices and more research indicates that this figure will be expected around 75 billion in 2025.This expectation requires additional dimension to the significance of IOT security. Thus, this paper demonstrates the evolution of security in IOT and Software.

Methodology. This paper reviews several related research works such as IoT security service and recent security approaches. There are various topics covered in recent security approaches such as blockchain-based technology, IoT Security Based on AI Techniques, Security of Cloud-based IoT Environment and so forth and so on. For reviewing recent studies, they consider a pie chart depicting the percentages of IoT security application domains from smart city with 8% and smart home with 23% to smart industry with 21%. there for this research focused on several recent research conducted in 2018-2019 mainly focused on IoT security. At the end it represents challenges and future direction such as limitation, heterogeneity, scalability of devices and trust management.

Findings. This paper approaches an appropriate manner as counter measurement, suggested by researchers to ameliorate

IoT security, like cloud-fog, lightweight algorithms, blockchain and machine learning. By and large, paper represents IoT security challenges as a future roadmap of researchers for novel research in this field. Challenges and issues such as lack of resources, vulnerabilities, and heterogeneity etc.
With regards to future direction and challenges in IoT development, this article represents several IoT security challenges defined by other researchers which could be assumed as a serious challenge in developing software and IoT.

[4] Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions

Motivations. a) To gain a greater understanding of the main applications and concept of IoT, b) To investigate the main challenges such as i) General challenges and ii) Unique challenges, c) To focus on Quality of service (QoS) which is a common factor between both general and special challenges and d) The possible solutions of recent research directions of IoT.

Methodology. MANET, "fault-tolerant routing" protocol, Midgar Software, Semantic Interoperability Architecture, BT, IP & GA, Aneka Hybrid cloud computing (private cloud + public cloud), IoT Virtualization Framework based on SenaaS technology, SMARTCAMPUS, CloudIoT Paradigm, Self-Organized Power Consumption Approximation (SOPCA) Algorithm, SCH.

Findings. a) Extensive review of IoT design and structure and the three dimensions of IoT (information items, independent network, and intelligent applications) which can address various issues (scalability, routing, networking etc.) and points out the differences between IoT and the traditional network

b) Identify all the main challenges (such as communication, networking, QoS, scalability, virtualization, big data, heterogeneity, and security) and provide the feasible solutions and indicate more related challenges to the IoT Environment.

1) Using MANET network, it's possible to improve Ad-hoc network as well as RFID (Radio Frequency Identification) and communication protocols to maintain connection between objects. 2) "fault-tolerant routing" protocol boosts the overall application range 3) Heterogeneity issue can be resolved by applying the graphic editor (Midgar Software) and will be able to maintain the scalability. 4) This architecture needs tools to enhance Interoperability so that accessing information could be done very quickly and efficiently to monitor it in the real world among physical objects 5) Implementation of BT algorithm to achieve higher Quality of Service (QoS) time. 6) Cloud computing technology will improve the scalability as well as to protect its privacy

7) Usage of SCH to strengthen and make sure the security of RFID system 8) Implementation of "IoT Virtualization Framework" will increase the overall performance of IoT 9) Showed some popular future IoT research applications (such as healthcare, smart city, smart grid, smart transportations, etc.) in the integration topic with cloud computing to provide a new dimension to control smart services and applications.

[5] Internet of Things: information security challenges and solutions

Motivations. a) to understand the progress and barriers of IoT foundations, b) to propose Security Intelligence approach to protect and secure IoT, c) to indicate few areas of future research to improve and provide higher scale of IoT environment.

Methodology. a) The author conducted a SWOT analysis to identify and prioritize its strengths, weaknesses, opportunities, and threats as per their network attacks and their taxonomy, b) Open Web Application Security Project (OWASP) to understand security issues.

Findings. a) Provides comprehensive complexity of vulnerabilities and attacks against IoT and identifies some key directions (such as IS - Information Security, is an essential segment of IoT, b) Implementation of blockchain technology in order to supply and access IoT data for security purposes, c) Deployment of IPv6, the most urgent security needs, so that IoT assets (hardware, software and all types of sensitive data to be protected) should be accessed at any location, d) Requirement of DPI (deep packet inspection) capability to manipulate IoT transport integrity, e) Virtualization through SDN (software-defined networking) to improve and better security so that issues like security breach could be identified and controlled promptly, f) Holistic approach helps to ease IS security risks of organizations.

[6] Software Evolution for Digital Transformation

Motivation. Today, there are many new business opportunities that make use of the potential of Internet-related digital technologies such as the Internet of Things, service computing, cloud computing, big data with analytics, mobile systems, collaboration networks, and cyber-physical systems. Organizations are currently transforming their strategies, cultures, processes, and information systems to become more digital. Digital transformation is transforming existing businesses and economies. Digitization facilitates the development of IT environments with small and distributed structures, such as the Internet of Things. This has a significant impact on the architecture of digital services and products. From a closed-world modeling perspective, the transition to more flexible open-world and living software and system architectures defines the moving context of adaptive and evolutionary software approaches that are essential to enable digital transformation. This article focuses on developing service-oriented software that supports digital transformation of digital services and products with microservices digital architecture.

Methodology. The paper explored the digital transformation of processes over a period of some days. Plots down an architecture of disintegrating enterprise services through a reference cube. The reference cube included Architecture Management, Architecture Governance, Information Systems Architecture, Security Architecture, Technology

Architecture, Operation Architecture and Business and Information Architecture. This reference cube was further used to federate through mini models and then comments on Software Evolution using the example of REST as a sample with Microservices.

Findings. The need for bottom-up integration of microgranular services was felt at the end of the paper. It was also observed that the Internet of Things and Microservices together influence the Digital Enterprise Architecture of Software Evolution and changed the way of modelling of complex systems in open world. It was later investigated that that current and next element of a service-oriented enterprise architecture to point to main influence factors, challenges, and research areas for the evolution of enterprise architecture and the evolving discipline of service computing. There is a need to integrate more analytics-based decisions support and context-data driven architectural decision-making. Limitations can be currently found, while integrating Internet of Things architecture in the field of multi-level evaluations of the approach of this paper, *as well as in domain-specific adoptions.*

[7]Current and Future Challenges of Software Engineering for Services and Applications

Motivation. Software is becoming increasingly prevalent in ICT (Information and Communication Technology), and it can no longer be regarded as a minor component of complex systems. It is the essential ingredient in sectors such as cloud, big data, IoT (Internet of Things), and CPS (Cyber-Physical Systems). A study needed to strengthen the software engineering discipline, which, despite its shortcomings, continues to grow.

Methodology. The paper is initially motivated by the need for reducing the Software Aging by specifically studying the challenges faced by European projects in Software Engineering. These included Software Design Challenges, Software Placement Challenges, Software Implementation Challenges, Software Design and Quality challenges while considering Orchestration of Middleware Challenges. The paper then compares all these challenges with the domain of Big Data and IOT.

Findings. On comparing the various challenges, the paper concludes by urging the need of accelerated open-source software innovation because most of the libraries are reused off open-source projects. The paper also stresses on the imperative requirement of software to improve itself through the big data gathered by large data sets. Introduction of AI/ML does make it easier for the software to evolve without a lot of hinderance. As time progresses the software will be able to port itself thanks to the data sets it gathers and the new migratable technologies that come.

b) Comparison among the reviewed papers

This section compares reviewed papers.

Paper	***Criteria 1 Focus area***	***Criteria 2 Method of research***	***Criteria 3 Practical example/Case Study***	***Criteria 4 Paper is based on***
The evolution in Software and programming language in IOT development	*General introduction about IOT and Software evolution, covering some points about the programming language used for IoT and the difficulties that developers may encounter with during development*	*Observation form industries and paper research and personal experience*	*Case Study*	*Comparing other articles and discussing about them*
IOT security evolution: Challenges and Counter Measurement	*Highlighting the main reasons that we need to be cautious about security in IoT and the relations between IoT and Software evolution and Security*	*Designing a pie chart for comparison purpose*	*Case Study*	*This paper reviews several related research works such as IoT security service and recent security approaches*
Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions	*General and special challenges, and points out to some future research directions for its solutions*	*Reviewed a set of popular applications in IoT*	*Practical Example*	*Researched on various challenges and its solutions*

Current and Future Challenges of Software Engineering for Services and Applications	*Focused on Software Aging through big data and cloud environment and self-evolving software through IOT and CPS.*	*Studied Software Aging in European projects*	*Derived conclusions by using Lean Six Sigma on European Companies*	*Research*
Software Evolution for Digital Transformation	*Focused on the changes in the rugged computer industry and the various strides taken to evolve different generation languages to cater to*	*Focuses on Microservices as a potential Future failsafe for evolution and breaking down of Software in IOT environment to ensure stable software extension*	*Measures the successes of implementing Microservices model*	*Research*
Internet of Things: information security challenges and solutions	*Aims at security challenges and attacks against the IoT and directs its counter measures with the help of Security Intelligence (SI) approach and propose some further prospective research directions.*	*SWOT analysis, comparing with the related work and numerous analogues*	*Case Study*	*Analyzed some methodologies and indicates some future solutions*

Table 1 Comparison among reviewed papers

Even the articles tackle different focus area, they show similar methods of search.

IV. FUTURE DIRECTIONS

A. 5 years

It's been anticipated that in the next 5 years, software IoT will grow much faster, but at the same time the world will face some serious issues due to higher cybercrimes attack. The best part is billions of IoT devices will be installed by 2027. This number points out that the future of IoT in next 5 years will be more advanced and innovative. 5G wireless network integration is expected to become double by 2026 that broadens a wide area in the cellular domain to provide a lightning speed and connects all the smart devices. This will boost 5G capabilities to fulfill consumer demand. On the other hand, as 5G networks are connected to the Wi-Fi router directly, it would become vulnerable easily and thus could be breached simply which is a major drawback that we are going to face soon. In contrast, Artificial Intelligence will continue to expand further from smart home hubs to lighting systems. It will be fully automated through machine learning in a way where it can process impromptu based on data received, without any external help from human beings. Moreover, the challenge of powering IoT devices in conjunction with the protection of the environment would force vendors to care more about developing energy-aware devices. This shift is already noticeable with Apple and its energy-aware ecosystem, where software and hardware are both optimized to save energy. Furthermore, common cross-manufacturers will provide a suitable way to enable universal machine-to-machine cooperation. With concern from a programmability viewpoint, a universal, containerized application-deployment and model supported across multiple manufacturers and industries will be possible. We can also think of an advent of possible cross-manufacturer programming APIs allowing generalized device discovery and data acquisition etc. Moreover, there will be dynamic remote programming and reprogramming of devices

B. *10 years*

Technological shift would redefine the way people perceive events how to efficiently use a given functionality. This could be an important improvement for energy consumption optimization. This would introduce new maintenance tasks such as research and development for instance. Furthermore, the democratization of IoT technology would lead to an interacting software development for IoT, not provided to developers today. The software and hardware would converge towards an agreed and worldwide used architecture. As a result, this would make software evolution easier (no longer need to deal with different platforms). For security, biometrics identification would be the number one software identification technology. Furthermore, healthcare IoT devices would be integrated in people's body. In this scenario, reliability would be the concern of software developers: a bug could kill a patient. This would redefine ethics and moral in software evolution: delivering a software system would take longer. There are some imperative issues that need to be considered in the future, the paramount of which is, limitation of device resources showing that classical security algorithms don't work well on IoT devices with limited capabilities. Furthermore, in terms of scalability of devices including the performance of IoT into existing systems which might lead to major difficulties in key management. Moreover, there are some great issues that we might encounter in the future such as privacy preservation, identity verification, trust management and so forth and so on.

V. *Conclusion*

Our research has provided software evolution challenges in IoT. The paper first identifies recent software evolution challenges, then draws future directions for the next 5 and 10 years. The main challenges are developing energy-aware software systems, protecting software from cyberattacks. On the other hand, it guides us by providing some proposed solutions for its key challenges to minimize the issues and improve the overall quality. To achieve this, Interoperability between devices needs to improve much more, and hence, the architecture needs the tools to develop the development and implement it successfully to monitor and update the information effortlessly.

Also, we speculate that the future of IOT depends highly on the capability of programming complicated and far-reaching topologies of IoT devices remotely. Once devices are connected to either public or private clouds, having sensor data and pervasive actuation capabilities, the concentration will switch from collecting data and analyzing them to application-programming ability to conserve complicated Real-world systems. Regarding actuation capabilities suggested by IoT devices from foundation for all this. They will provide us with a suitable manner to command-and-control daily objects in our environment from the convenience of a programming environment or an application in front of us.

VI. References

[1] S. X.-d.-S. a. K. E. K. Georgiou, "The IoT Energy Challenge: A Software Perspective," *IEEE Embedded Systems Letters,* vol. 10, no. 3, pp. 53-56, 2018.

[2] A. T. a. T. Mikkonen, "A Roadmap to the Programmable World: Software Challenges in the IoT Era," *IEEE Software,* vol. 34, pp. 72-80, Jan.-Feb 2017.

[3] A. M. A. Abuagoub, "IoT Security Evolution: Challenges and Countermeasures Review," 2019.

[4] Z. &. A. H. &. B. M. Hassan, "Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions," *International Journal of Computer Applications,* 2015.

[5] N. T. A. Miloslavskaya, "Internet of Things: information security challenges and solutions," *Cluster Comput,* vol. 22, pp. 103-109, 2019.

[6] R. S. J. B. D. J. a. M. M. Alfred Zimmermann, "Software Evolution for Digital Transformation".

[7] C. C. P. D. E. D. N. P. G. S. K. V. S. A. S. V. V. A. Z. Z. Z. Giuliano Casale, "Current and Future Challenges of Software Engineering for Services and Applications,," *Procedia Computer Science,* vol. 97, pp. 34-42, 2016.

[8] J. V. D. V. P. a. R. H. A. P. Suresh, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," *International Conference on Science Engineering and Management Research (ICSEMR),* 2014.

[9] M. Cube, "Never miss taking a pill again," 2022. [Online]. Available: https://www.medacube.com. [Accessed March 2022].

[10] M. K. L. C. W. M.-L. T. Jianxin Wang, "The evolution of the Internet of Things (IoT) over the past 20 years," *Computers & Industrial Engineering,* vol. 155, 2021.

[11] A. H. Hussein, "Internet of Things (IOT): Research Challenges and Future Applications," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 10, no. 6, 2019.

[12] M. &. S. D. &. S. S. Khuntia, " Impact of Internet of Things (IoT) on 5G," 2021.

VII. Contributions

ID	*Name*	*Contributions*
40184906	*Saswati Chowdhury*	*Reviewed paper: [4], [5]* *Focus area: Abstract, Future Directions, Conclusions*
40197899	*Sepehr Seifpour*	*Reviewed paper: [2], [3]* *Focus area: Background, future Directions, conclusion*
40171011	*Gilles Schneider*	*Reviewed paper: [1]* *Focus area: Abstract, Introduction, Background, Future directions.*
40197697	*Vaibhav Sharma*	*Reviewed Paper: [6], [7]* *Focus Area: Introduction, Background, Future Directions*